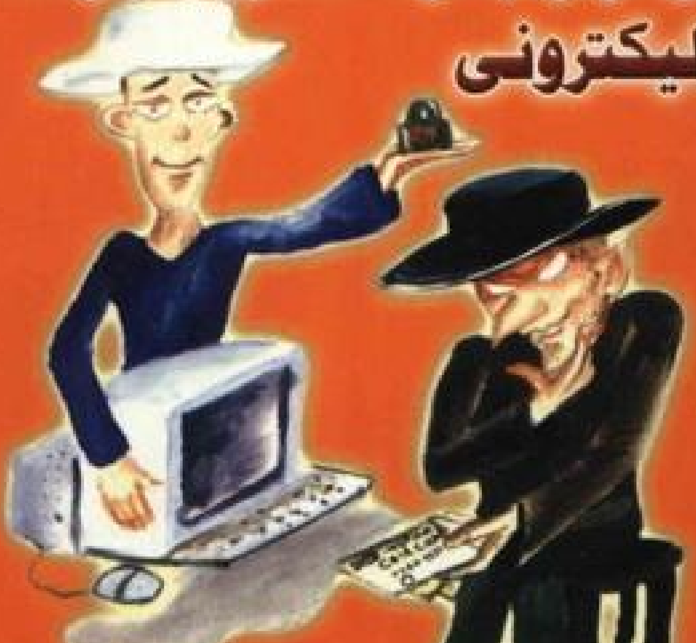
موسوعة التجارة الإليكترونية 12

أمن المعلومات والمواقع وأجهزة الكمبيوتر والدفع الإليكترونى



كيف تؤمن نفسك واولادك من الهاكر والكراكر

كيف تتخلص من الفيروسات

خالد محمد خالد
KHALED MOHAMED KHALED
Internet specialist diploma

بسم الله الرحمن الرحيم

نرفع درجات من نشاء وفوق كل ذي علم عليم

صدق الله العظيم

إعداد

خالد محمد خالد

بكالوريوس العلوم – جامعة الإسكندرية
ودبلوم الدراسات العليا في الإنترنت
من الولايات المتحدة الأمريكية

Khaled Mohamed Khaled

Internet and ecommerce specialist Diploma

Washington D.C., USA

المركز العلمي لتبسيط العلوم

٢٣ حسن رفعت، سيدي بشر، إسكندرية، مصر

تليفون: ٥٢٩٨٤٢٨ — فاكس: ٥٢٩٨٤٢٨

بسم الله الرحمن الرحيم

(فمن يعمل مثقال ذرة خيراً يره،
ومن يعمل مثقال ذرة شراً يره)

صدق الله العظيم

إعلم اخى العزيز ان ديننا الحنيف حذر بعدم الإضرار بالناس إن كان في ارزاقهم او فى علمهم او فى انشطتهم ولا تكن من ذوى النفوس الضعيفة فهم جاهلون بأن الله هو الرقيب وإنه سبحانه وتعالى ليس بظلام للعبيد .

فيمكنك أن تكون هاكر بل وكراكر ولكن فى سبيل الله ، ما بالك إذا إستخدمت كل ما لديك من علم و فنون وتقنية فى غلق المواقع الإباحية وتتبع اسرار العدو ، أليس ذلك فى سبيل الله.

قال تعالى : *"واما تخافن من قوم خيانة فانبذ إليهم على سواء إن الله لا يحب الخائنين" سورة الأنفال الآية ٥٨*

موسوعة التجارة الإليكترونية (١٢)

أمن المعلومات

Information Security

رقم الإيداع بدار الكتب : ٢٠٠٦/٢١٤٠٢

ISBN: 977-6197-28-0

رجاء

رحمه الله والدى ... قال لى ذات يوم
لكل شىء زكاة وزكاة العلم تبليغه للآخرين ..
اللهم إن كان هذا الكتاب فيه منفعة للأمة العربية فاجعله
فى ميزان حسنات والدى .. وبهذا العمل أدعو الله سبحانه وتعالى
ان ينصر المسلمين فى كل بقاع الارض
وأن يخلص الأقصى المبارك من أيدى اليهود ...

شكر وتقدير

جزى الله خيراً كل من ساعدني في إتمام هذا العمل المتواضع ليضع نور الأمل
داخل عيون إخواني وأخواتي مستخدمي شبكة الإنترنت....

تمهيد

لقد إعتمدت إعتماداً كلياً فى كتابة هذا الكتاب على خبرتى المكتسبة فى
مجال العمل عبر شبكة الإنترنت طوال إحدى عشر عاماً
وفى خلال هذه الفترة واجهت الكثير من المشاكل الأمنية والإختراقات
للمواقع وللأجهزة وللشبكات ، لذلك أردت بهذا الكتاب أن أوضح
ما هى المشاكل الأمنية وما هى أنسب الحلول حتى نتجنب عمليات الإختراق
والسرقة وخصوصاً أمن عمليات الدفع عبر الشبكة
ولقد قمت بالإستعانة ببعض الكتب الإليكترونية **e-book** بالمواقع
العربية والمواقع الأجنبية وقمت بإعادة صياغة بعضها علمياً لكى يتماشى
مع بلادنا العربية وما يحدث لمواقعنا من إختراقات لذلك أشكر أصحاب
هذه المواقع ..

لذلك محتوى الكتاب يعبر عن رأى المؤلف فى هذا المجال ،
بدون أدنى مسؤلية على الناشر.

المقدمة

حينما أصبحت ضحية الهاكرز كتبت هذا الكتاب

١. حينما كنت فى أمريكا وأثناء عملى بموقع ebay وهو موقع مزاد للبيع والشراء كما تعلمون ، إخترق أحد الهاكرز ذات القبعة السوداء (الكراكرز) البريد الإليكترونى الخاص بى وسرق كلمة السر وإسم المستخدم وبالتالى قام بسرقة إسم المستخدم وكلمة السر بحسابى بموقع ebay ، كل هذا وأنا لا أدرى إلا بالصدفة البحتة ، حينما أفتح بريدى لا أجد أية مراسلات من العملاء ، الغريب أننى أذهب إلى ebay وأرى منتجاتى قد بيعت ولكن لا أستقبل أية مراسلات تفيد ذلك ، لم يكن فى الحسبان أن وراء هذا الحدث هاكرز يهود وقد عرفتهم بعد ذلك ، فقد أرادوا إنهاء عملى بموقع ebay وسرقتى حتى أتوقف عن منافستهم ويقوموا هم فقط بالبيع عبر الشبكة. لم يكتفوا فقط عند إغلاق موقعى بل قاموا بإدراج مئات المنتجات تحت إسمى وفى خانة مواصفات الدفع كتبوا أنهم يقبلون الدفع باستخدام الشيكات والحوالات money order ولكن

الحمد لله تم إكتشاف هذا اللعبة ثم أسرعت وأبلغت **ebay** عن طريق **Live Chat** وهى الأسرع للإبلاغ عن السرقات والنصب وبالفعل تم إغلاق حسابي فوراً ، ثم قامت شركة **ebay** بفتح حسابي من جديد مع تغيير إسم المستخدم وكلمة السر .. وقد أوقعت بهم بحمد الله ورسمت لهم خطة قانونية وليست إجرامية كما فعلوا ، فقط قمت بقراءة سياسات موقع **ebay** جيداً وإكتشفت ثغرة هامة يمكن عن طريقها الإيقاع بأى مستخدم وغلق حسابه فوراً ، هذه الثغرة تسمى **shell bidding** وهذه عملية يقوم بها صديقان لهما حسابين مختلفين بموقع **ebay** يقوم إحداهما بالمزايدة على منتج الآخر حتى يكثروا من مبلغ المزايدة وهذه العملية إن تم رصدها بواسطة قسم الأمان والتأمين بموقع **ebay** فسوف يتم غلق الحسابين فوراً ونهائياً و بلا رجعة ، وقد كان ، فقد قمت بمراقبتهم وكنت أنا **third party** بينهم حتى تكتمل القضية ، وأبلغت **ebay** بأننى أحاول أن أشترى منتج من هذا المستخدم ولكن يوجد مستخدم آخر يرفع فى القيمة لحساب المستخدم الأول وتكررت هذه العملية مرات عديدة وتم رصدهم وتم إغلاق حسابهما نهائياً .. فإن كنت أنا فى هذه الحالة هاكر فأنا هاكر ذات قبعة بيضاء قمت بإبلاغ الهيئات

المختصة عن جريمة بشعة وهى جريمة السرقة التى يعاقب عليها بقطع اليد فى مذهبنا الحنيف ..

*ومن هنا أنصح جميع الإخوة والأخوات العرب الذين يمكثون فى البلاد المدرجة للعمل بـ **ebay** و **paypal** كأمريكا وأوروبا وبعض دول آسيا وأستراليا وبالطبع كندا ، أن يتوخوا الحذر حين التعامل عبر مواقع **ebay** و **paypal** لأنها أكثر المواقع إختراقاً بالرغم من وجود برامج حماية شديدة ...*

٢. **إقتحام موقع المركز العلمى لتبسيط العلوم عن طريق دار نشر معروفة بالإسكندرية وتغيير الموقع إلى موقع آخر لمدة ساعتين ثم تيقظوا لها موظفى المركز وأغلقوا الثغرة وهو الآن يعمل بحماية جدار نارى والحمد لله ، وقد تم معرفة الهاكرز ونحن الآن نقاضيهم وسيتم الإفصاح عنهم عن قريب .**

٣. ذهبت إلى أحد البنوك بالإسكندرية لفتح حساب وأودعت مبلغ معين لفتح الحساب ، وبعد أسبوعين أودعت مبلغ آخر لغرض تحويله إلى مصدر بالخارج ، وبعد شهر أرسل البنك كشف الحساب فوجدت أن الحساب ينقصه مبلغ آخر لم يتم إضافته ، ذهبت إلى البنك لأتحسس الأمر وأسأل عن ما حدث

، فوجدت موظفى البنك فى ذهول وأحسست أن شيئاً ما يجرى وتعالت أصوات الموظفين وأرسلوا إلى قسم الكمبيوتر والمسؤولين عن حماية حساب العملاء وقد كان ما فى الحسبان ، لقد إخترق هاكرز حسابات البنك وأخذ مبالغ من حسابات العملاء وتم غلق النظام لمدة يومين لحين سد الثغرات ، وبالطبع تم إسترداد المبلغ الذى سرق من حسابى ...

٤. أرسل أحد أعداء النجاح شخصاً إلى مكتبى وبطريقة ما إكتسب ثقتى به حتى أنه قال لى إسمح لى أن أقدم لك هدية على جهاز الكمبيوتر الخاص بك ، فقلت له لا مانع تفضل وجلس أمام الجهاز وللأسف وضع المجرم دودة أو أعتقد كانت تروجان وتم بهذا البرنامج التعرف بل وسرقة كل ملفات الكتب الموجودة لدىّ بالجهاز ولم يكتفى بذلك بل وقد دمر الجهاز كليةً حتى وصل للوضع فورمات **format** والحمد لله كان لدى نسخة أخرى من الكتب على **CD** ، وبعد إكتشافى لهذا العمل الإجرامى لم أتخيل أن هناك شباب المفروض أنهم حماة الوطن ، هم بالفعل من سيدمر الوطن وهذا ما نراه بالفعل بين أوساط الشباب بنين وبنات ، معظمهم هاكرز ذات قبعة

سوداء .. لذلك لا تسمح أبداً لأى صديق قبل العدو أن يجلس على جهازك أو تعطيه كلمات السر الخاصة بك .

٥. فى هذه الأيام حدثت لى حادثة غريبة جداً : أرسل لى أحد العملاء أنه يريد شراء موسوعة التجارة الإليكترونية ، فقمت بالرد عليه ورحبت به وقلت له أرسل العنوان الخاص بك وسوف أرسل الكتب بطريقة **COD** الدفع عند الإستلام، وبالفعل أرسله لى وهو يقيم بإحدى قرى مصر ، أرسلت الكتب واستلم الكتب ودفع قيمة الموسوعة .. دخلت إلى بريدى الإليكترونى الخاص ببيع الكتب فوجدت رسالة يقول لى لماذا تبيع الكتب بدون أن يدفع الزبون قيمة الشحن
وأحسست أنه يقولها بنية لم ترضنى ، والله أعلم .. دخلت إلى بريدى الخاص بالرد على إستفسارات أعضاء المنتدى فوجدت رسالة من هذا العميل بها مرفقات فتحت الرسالة ولكن ظهرت لى رسالة من برنامج الحماية الخاص بى يقول أن هذه الرسالة بها فيروس مدمر وطبعاً قمت بغلق الرسالة ولم أفتحها .. فدخلت إلى بريدى الثالث الخاص بالدعم الفنى للعملاء فوجدت رسالة أيضاً من هذا العميل بها مرفقات عبارة عن صور وطبعاً كانت مليئة بملفات التجسس وطبعاً لم أفتحها .. فى الحقيقة لم أنام حتى

الآن لكى أعرف ما هى الثغرة التى دخل منها هذا العميل وأخذ الإيميلات **E-mails** الخاصة بى ، غريب جداً ، وفى النهاية إكتشفت أن هذا العميل الذى إشترى الموسوعة أرسل لى برنامج تجسس و هذا البرنامج يرسل له جميع الحروف التى تكتب على لوحة المفاتيح الخاصة بى فعرف الإيميلات الخاصة بى من هذا الملف والله أعلم ربما يكون قد عرفها عن طريق إختراقات أخرى .. وبالطبع ما كان علىّ إلا أن غيرت كلمات السر الخاصة بالإيميلات الثلاثة ..وأنا الآن أحاول التأكد من طريقة الإختراق قبل فعل أى إجراء قانونى ضد هذا الكراكر ..

٦. أحد أصدقائى سرق هاكرز رقم بطاقته الإئتمانية واشترى موبايل (جوال) ولم يتم الحصول على مكان الهاكرز .

٧. أحد الهاكرز تلصص إلى جهاز كمبيوتر أحد أصدقائى وكشف عن ملفاته وصوره ثم أخبره أن لديه ملف تجسس ولصدق كلامه قال له ما هى الملفات الموجوده بجهازه.

٨. لا تترك كاميرا الويب مفتوحة طوال الوقت حيث أن بعض الهاكرز يدخلون جهازك وينتهزون فرصة وجود الكاميرا

مفتوحة فيشاهدونك ، فعلى الأخوات الإنتباه إلى ذلك لأنه بالفعل تم رؤية الفتيات عن طريق برامج إختراق الملفات ...

٩. وأقوى ضحايا الهاكرز والكراكرز هم المساهمين فى البورصة والأسهم وما حدث ببورصة السعودية الأيام الماضية من هبوط شديد ما هو إلا بسبب إختراق الهاكرز اليهود لأنظمة البورصة السعودية والتلاعب فيها فكانت السبب فى إنهيارها ولكن تم السيطرة عليها ..

١٠. أتسلم كل يوم عشرات الرسائل الإليكترونية من أسماء لا أعرفها وبالطبع لا أقوم بفتحها لأنها جميعاً تحتوى على فيروسات إلا فئة قليلة قد تكون صادقة وهى تعرض إعلاناتها وخدماتها عبر بريدك الإليكترونى. لذلك لا تقوم بفتح الرسائل الغامضة .

١١. سألنى صديقى هل لى أن أخترق أجهزة الكمبيوتر وأحذف المواقع والصور الفاضحة ، قلت له يمكنك ذلك بالرغم من أنك فى هذه الحالة تعتبر هاكر ذات قبعة بيضاء ، فضحك.

١٢. ثم سألنى وهل لى أن أخترق أى موقع جنسى وأقوم بإغلاقه ، قلت له نعم وأنت فى هذه الحالة تجاهد فى سبيل الله ..

١٣. وتابع هل الإختراق والتجسس جريمة يحاسب عليها القانون ، قلت بالتأكيد يعد الإختراق والتجسس جريمة يحاسب عليها

القانون وذلك في الكثير من دول العالم حتى أن كل دولة الآن لديها جهاز خاص بمكافحة الإجرام عبر الإنترنت .. فلا تستغرب عزيزى القارىء حينما ترى الهاكر والكراكر بجوار القاتل ومروج المخدرات واللصوص فى زنزانة واحدة ولكن الفرق بينهما هو أن القاتل إذا خرج وجد الدنيا سوداء وجميع الأبواب مغلقة أمامه ، أما بمجرد خروج الهاكر أو الكراكر من السجن يجد استقبالاً حافلاً من الشركات العالمية الكبرى التي تسارع إلى توظيف الهاكرز بغرض الاستفادة من خبرهم في محاربة الهاكرز وكذلك للاستفادة من معلوماهم في بناء برامج وأنظمة يعجز الهاكرز عن إقتحامها.

١٤. الخبر الأكيد أيضاً أن الهاكرز والكراكرز أصبحوا من أقوى الوسائل التى يستخدمها المنظمات الإستخبارية كالموساد الإسرائيلى والـ FBI الأمريكى لسرقة معلومات العدو وتدمير وتغيير مواقعهم بالويب كما هو الحال فى كثير من المواقع الدينية التى غيرها أعداء الله إلى مواقع جنسية.

١٥. إذاً الحروب الإليكترونية هى حروب هذا العصر وليست حروب ساحات القتال.

١٦. و يجب أن نؤمن بأنه لا يوجد نظام تشغيل أو جهاز بدون ثغرات أو منافذ يستطيع من خلالها الهاكرز أو الكراكرز

الإختراق ، لأنه فى الحقيقه الهاكرز هم بالفعل من قام بتصميم هذه الأجهزة سواء كان بالفكرة أو بالتصميم أو عمل البرامج أو حتى بالإستشارة التقنية ، فأغلب وأقوى الهاكرز في العالم هم بالفعل مبرمجون ومهندسون للكمبيوتر والاتصال والشبكات.

١٧. وأخيراً الشباب ، الشباب ، الشباب المراهقون ، الذين يظنون أنهم يغامرون ويلهون فقط بهذه الأعمال التى لا يظنون أنها أعمال إجرامية ، لابد من إيقافهم وعدم مساعدتهم فى التلصص والتجسس والسرقة حتى لا نراهم يوماً بين القضبان .

*يقول الله تعالى: " **ولا تجسسوا** ولا يغتب بعضكم بعضا أيحب أحدكم أن يأكل لحم أخيه ميتا فكرهتموه واتقوا الله إن الله تواب رحيم "*

سورة الحجرات الآية ١٢

واعلم أخى الشاب أن إستخدام العلم فى الضرر بالناس خيانة وقد قال الله سبحانه وتعالى :

*" واما تخافن من قوم **خيانة** فانبذ إليهم على سواء إن الله لا يحب **الخائنين**"*

سورة الأنفال الآية ٥٨

وبالطبع الهاكر أو الكراكر خائن لا يحبه الله ..

وفى سورة القصص الآية ٨٣ يقول الله سبحانه وتعالى:

"تلك الدار الآخرة نجعلها للذين لا يريدون علوا في الأرض ولا فسادا والعاقبة للمتقين"

وفى سورة المائدة الآية ٣٣يقول الله تعالى

" إنما جزاء الذين يحاربون الله ورسوله ويسعون في الأرض فسادا أن يقتلوا أو يصلبوا أو تقطع أيديهم وأرجلهم من خلاف أو ينفوا من الأرض ذلك لهم خزي في الدنيا ولهم في الآخرة عذاب عظيم"

أما فى حق السارق والسارقة قال تعالى

" والسارق والسارقة فاقطعوا أيديهما جزاء بما كسبا نكالا من الله والله عزيز حكيم"

سورة المائدة الآية ٣٨

الفصل الأول

مصطلحات امن المعلومات والمواقع والحاسبات

قبل البدء فى شرح مادة هذا الكتاب لابد أن نـذكر بعـض المفـاهيم والمصطلحات التى سنتناولها طوال فصول الكتاب القادمة ، فليس مـن الحكمة أن نذكر علاج ووقاية قبل أن نعرف المرض وكيفيـة توغلـه داخل الجسم حتى نتمكن من التخلص منه ، من مصدره (جذوره) .

فإذا أردت أخى القارىء أختى القارئة أن تتمكنوا من حماية أجهـزتكم ومواقعكم من الإختراق والدمار فلابد أن تتعلموا هـذه المصـطلحات أولاً حتى تعرفوا ما هو أصل العطب **fault** وحتى يمكنـك سـرعة المعالجة فور حدوث المشكلة أو بمعنى آخر فور الإصابة بالفيروس .

فلا يجوز أن ندخل فى فصل كيفية الحماية قبل أن نتعرف مـثلاً علـى معانى هامة مثال : الهاكر و الكراكـر ومعـنى الفـيروس والـدودة والتروجان وأيضاً مضادات الفيروسات مثال نورتون ..

لذلك فى الفصل القادم نتعرف وندرس بعض المفاهيم الخاصة بأمن

المعلومات والمواقع وحماية أجهزتنا من الإختراق والثغرات والفيروسات وبذلك نكون قد جهزنا أنفسنا للدخول فى فصول الكتاب وفهم مواضيعها بكل سهولة ويسر .

– Administrator المدير

شخص يقوم بإعداد مصادر الشبكة وتسجيل المستخدمين وأرقامهم السرية وصيانة المصادر .

- Agent عميل

في نظام العميل/الموفر(الخادم) **(Client/Server)** ، ذلك الجزء من النظام الذي ينفذ عملية إعداد وتبادل المعلومات نيابة عن برنامج المضيف **Host** أو الموفر **Server**

- Alert تحذير

تقرير عن وجود خطأ بشكل علامة أو نافذة تحذير أو صوت يطلقه الكمبيوتر للتنبيه .

- ASCII قاعدة المعايير الأمريكية لتبادل المعلومات

American Standard Code for Information Interchange

معيار لتحويل الأحرف إلى أرقام وتحتوي على سبعة جزيئات بقيمة ثنائية

تتراوح بين الصفر و ١٢٧ .

- Anonymous مجهول

تم استخدامه كإسم مستخدم للدخول على بعض أجهزة الكمبيوتر البعيدة .

- Authentication التوثيق

تعريف هوية شخص أو الإجراءات الخاصة بذلك .

- Band Width عرض النطاق

هي كمية المعلومات التي يمكنك إرسالها على خط معين في وقت محدد. عرض النطاق يقاس بعدد النبضات في الثانية **Bits per Second** وتكتب **(bps).**

- BBS لوحة إعلانات النظام

كمبيوتر مزود ببرامج معينة يوفر رسائل إليكترونية وملفات إضافية للخدمات الأخرى .

- Binary ثنائي

وسيلة عد تستخدم الرقمين ٠ و ١ ، وهي الوسيلة التي يعمل بها الكمبيوتر داخلياً، وتحتوي الملفات الثنائية على ثمان جزئيات تتراوح بين صفر و ٢٥٥

- Browser المتصفح

برنامج التصفح يستخدم للإبحار داخل شبكة الإنترنت **WWW**

- Client تابع

جهاز كمبيوتر يقوم بطلب الخدمة من جهاز كمبيوتر آخر، فعندما يطلب كمبيوتر اشتراك مع مزود خدمة **ISP** فإنه يعتبر تابع لمزود الخدمة **(Client of ISP).**

– Compression ضغط

عملية ضغط المعلومات لتخزين الملف في مساحة أصغر .

– Connection ربط

وسيلة إتصال بين جهازي كمبيوتر .

- Crack تخريب

مصطلح يطلق على برنامج يقوم بفك شفرة أحد البرامج المشتركة وجعله مجاني .

– Cracker مخرب

شخص يحاول الدخول على نظام ما دون تصريح ويسبب له أضرار .

- Data بيانات

معلومات وبشكل خاص المعلومات المستخدمة بواسطة البرامج، أصغر وحدة

في المعلومة يمكن للكمبيوتر فهمها هي **bit**

- Default بديل افتراضي

قيمة أو فعل أو ترتيب إفتراضي يقوم الكمبيوتر بافتراضه في حال عدم قيام المستخدم بإعطاء تعليمات صريحة بخلاف ذلك.

- Device جهاز

الأجزاء التي يتركب منها الكمبيوتر **Hardware** مثل الشاشة والطابعة وخلافه ، هذه الأجزاء يمكن أن يطلق عليها أيضاً الأجزاء الخارجية **Peripheral** لأنها منفصلة بصورتها المادية عن الكمبيوتر ولكنها مربوطة به .

- Dial-up اتصال

استخدام التليفون لربط الكمبيوتر بالانترنت عبر فاكس مودم. وهذا يعني أنه كي تحصل على الخدمة فإنه عليك أن تعمل مكالمة هاتفية .

-Digital Certificates الشهادات الرقمية

تصدُر الشهادات الرقمية عن الجِهات المانحة (**certificate authorities- CA**) الموثوق بها التي توقّع عليها، وتُستَخدَم هذه الشهادات للتحقُّق من موثوقية المفاتيح العامة التي أُصدِرَت.

وفي البداية، يقوم شخص (أو شركة) بتوليد زوج من المفاتيح العامة/الخاصة،

ثم يُرسَل المفتاح العام إلى جهة مانحة للشهادة (CA). وتُضيف الجهة المانحة (CA) بعضَ المعلومات المتعلّقة بالشهادة (مثل: الاسم، ورقم التعريف (.No ID)، وعنوان البريد الإلكتروني (Email address)، وتاريخ الانتهاء (date expiration)، والرقم التسلسُلي (. serial no))، وتُوقِّع عليها بالمفتاح العام لطالب الشهادة، وبالمفتاح الخاص للجهة المانحة للشهادة (CA). ويصادِق توقيع الجهة المانحة للشهادة (CA) على المعلومات المُضافة إلى الشهادة وعلى المفتاح العام الموجود ضمن الشهادة. ويمكن أن ترسِل الجهةُ المانحةُ الشهادةَ إلى طالبها، أو تنشرَها للعموم، أو تحتفظَ بها في خادم الشهادات (certificate server) (قاعدة بيانات تسمح بتسليم واسترجاع الشهادات الرقمية).

- Domain حقل

هو ذلك الجزء من الــ DNS الذي يحدد مكان شبكة كمبيوترك وموقعها في العالم .

- DNS نظام اسماء الحقول

Domain Name System هو نظام لتحديد العناوين بالشبكة IP Addresses المطابقة للكمبيوترات المسماة والحقول ..Domains الــ DNS يتكون من سلسلة من المعلومات تفصل بينها نقاط... خدمة أسماء الحقول Domain Name Service هي عبارة عن برنامج يقوم

بتحويل أسماء الحقول **Domain Names** إلى عناوين شبكية **IP Addresses.**

-Digital Signature التوقيع الرقمي

يُستَخدَم التوقيع الرقمي للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل .

ويمكن للمرسِل استخدام المفتاح الخاص لتوقيع الوثيقة إليكترونياً. أما في طرف المستقبِل، فيتم التحقّق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب.

-Electronic Mail البريد الاليكتروني

يرمز له **e-mail** وهو نظام يمكن بموجبه لمستخدم الكمبيوتر تبادل الرسائل مع مستخدم آخر أو مجموعة مستخدمين بواسطة شبكة الإنترنت، ويحتاج البريد الاليكتروني إلى برنامج بريد مثل **Outlook** :أو **Eudora** ليتمكن من الارسال أو يعمل تحت برامج مجانية لمواقع مثل **yahoo** .

-Emotion رموز المشاعر او الاحاسيس

رموز تستخدم للتعبير عن المشاعر على الانترنت مثل إبتسامة ، غضب ، حزن ، سعادة

- Encryption التشفير

هو معالجة كتلة من المعلومات بهدف منع أي شخص من قراءة تلك المعلومة باستثناء الشخص المقصود إرسالها إليه، وهناك العديد من أنواع التشفير .

و يُعرّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة.

- FAQs الاسئلة المتكررة

Frequently Asked Questions وثيقة على الانترنت الغرض منها فحص وتدقيق المعلومات التي يحتاج إليها الكثير من الأشخاص بصفة متكررة .

- Firewall جدار نار

نظام تأمين لتقييد عملية الدخول على أجهزة الكمبيوتر الموجودة على شبكة محلية **LAN** من أي مكان في الخارج .

- Flame التطهير

ردة فعل غاضبة لرسالة تم نشرها على **Usenet** أو القوائم البريدية **Mailing List** أو لوحات النقاش **Message Boards** ، التطهير يحدث لعدة أسباب مثل تعميم رسالة على الانترنت أو طرح سؤال توجد

إجابته في الـــ FAQs ، حرب التطهير قد تحدث عندما يرد شخص تعرض للتطهير على الرسالة أو الرسائل التي وصلته .

- Gateway بوابة

مصطلح بوابة **Gateway** البوابة هي أداة أو برنامج اتصال يقوم بتسيير المعلومات من شبكة إلى أخرى .

- Gopher خدمة جوفر

نظام طورته جامعة مينيسوتا الأمريكية بهدف تسهيل عملية استخدام الانترنت وهو يعتمد على عملية البحث من خلال القوائم لقراءة الوثائق ونقل الملفات **Gopher** يمكنه الإشارة الى الملفات ومواقع **Telnet** ومراكز معلومات **WAIS** وغيرها .

- Hacker متطفل

المتطفل هو الشخص الذي يشعر بالفخر لمعرفته بطرق العمل الداخلية للنظام أو الكمبيوتر أو الشبكات بحيث يسعى للدخول عليها دون تصريح .

- Host مضيف

غالباً ما يستخدم مصطلح مضيف **Host** للكمبيوتر الذي يتيح للمستخدمين الدخول عليه .

- HTTP بروتوكول نقل النص التشعبي

HTTP هي وسيلة تجعل من الممكن التصفح عبر وثائق الشبكة العنكبوتية، المستخدم يضغط على وصلات ربط موجودة على وثيقة الشبكة العنكبوتية مما يمكنه من الذهاب إلى تلك الوثيقة حتى لو كانت موجودة على جهاز آخر .

- ISDN الشبكة الرقمية للخدمات الموحدة

Integrated Services Digital Network هي تكنولوجيا جديدة تحتوي على شبكات صوتية ورقمية في وسيلة واحدة وتعتبر خدمة اتصالات فائقة السرعة ولكن وجود **DSL** حجم من استعمالها .

- IP بروتوكول الانترنت

Internet Protocol هو طبقة الشبكة الخاصة ببروتوكول **TCP/IP**والتي تستخدمها الأدوات على الانترنت للاتصال ببعضها. والـ **IP Address** عنوان بروتوكول الانترنت، هو العنوان الخاص بكل كمبيوتر متصل بشبكة ولكل عنوان الـ **IP** طريقتين للكتابة اما رقمية **(TCP/IP Address)** مثل ١٩٢,١٦٨,٢٣,١ أو حرفية **(FQDN)** وهي العناوين التي نكتبها عادة في المتصفحات مثل **ftp.books4internet.com** والعنوان الحقيقي هو الرقمي ولكن لصعوبة حفظه فنكتب العنوان الحرفي ولكن في الشبكة داخلياً يتم ترجمة العنوان الحرفي الى العنوان الرقمي المطابق له .

- ISP مزود خدمة الانترنت
- Internet Service Provider هو الشركة التي يقوم المستخدم - عادة – بالاشتراك لديها للحصول على ربط بالانترنت، وهذه الشركة مرتبطة بالانترنت مباشرة من إحدى الشركات الأعضاء في CIX

JPEG
وسيلة لضغط الصور المستخدمة في الانترنت ويكون إمتداد إسم الصورة هو .jpeg

- Kilobit كيلو بت
وحدة قياس تعادل ١٠٢٤ ب، وتستخدم عادة في تحديد الطاقة الاستيعابية للذاكرة

- Kilobyte كيلو بايت
وحدة قياس تساوى ١٠٢٤ بايت .

- Layer طبقة
شبكات الكمبيوتر قد تنظم على شكل مجموعة أعداد أكثر أو أقل من البروتوكولات المستقلة كل منها في طبقة Layer وقد تسمى مستوى Level.

- Login تسجيل

أي أن تقوم بتسجيل إسمك كمستخدم لنظام أو شبكة فيصبح لديك اسم مستخدم **Login Name.**

- Log off انهاء عملية التسجيل

هو إخبار النظام بأنك أنهيت عملك وستقطع الإتصال.

– Lurking التواري

يستخدم هذا المصطلح للتعبير عن شخص ليس لديه مشاركة نشطة في مجموعة الاخبار او لوحة النقاش أو قائمة البريد التي اشترك معها، ويفضل التواري للأشخاص المبتدئين الذين يريدون التأقلم في البداية مع الآخرين

- Mailing List قائمة بريدية

قائمة بعناوين اليكترونية لعدة أشخاص. كل شخص مشترك في هذه القائمة يرسل موضوعاً يخص اهتمامات هذه القائمة الى كمبيوتر رئيسي يقوم بتحويل هذه الرسالة الى جميع المشتركين في القائمة البريدية، هناك قوائم معدلة **Moderated** وتعني أن الرسالة ترسل في البداية الى صاحب هذ ه القائمة ليدقق فيها وإذا تأكد من صلاحيتها يقوم بارساله للبقية وهناك قوائم غير معدلة **Immoderate** وتقوم بارسال الرسالة أتوماتيكياً للمشتركين .

- Megabyte ميجا بايت

وحدة قياس تعادل ١٠٢٤ كيلو بايت أو ١٠٤٨٥٧٦ بايت .

- MIME توصيلة بريد الانترنت المتعددة الأغراض

Multipurpose Internet Mail Extension نظام لتوفير القدرة على نقل البيانات غير النصية كالصور والصوت والفاكس من خلال البريد الالكتروني .

Message digests البصمة الإليكترونية للرسالة

رغم أن التشفير يمنع المتلصّصين من الاطلاع على محتويات الرسالة، إلا أنه لا يمنع المخرِّبين من العبث بها؛ أي إن التشفير لا يضمن سلامة الرسالة **(integrity).** ومن هنا ظهرت الحاجة إلى البصمة الإليكترونية للرسالة **(message digest)**، وهي بصمة رقمية يتم اشتقاقها وفقاً لخوارزميات معيَّنة تُدعى دوالّ أو اقترانات التمويه**(hash functions)** ، إذ تطبِّق هذه الخوارزميات حسابات رياضية على الرسالة لتوليد بصمة (سلسلة صغيرة) تمثِّل ملفاً كاملاً أو رسالة (سلسلة كبيرة). وتُدعى البيانات الناتجة البصمة الإليكترونية للرسالة.

MD2, MD4، MD5 خوارزميات البصمة الإليكترونية

طوَّر رونالد رايفست (**Ronald Rivest**) خوارزميات <u>**MD2**</u> و <u>**MD4**</u> و <u>**MD5**</u> الخاصة بالبصمة الإليكترونية للرسالة. وهذه

الخوارزميات هي اقترانات تمويه يُمكن تطبيقها على التواقيع الرقمية. وبـدأ ظهور هذه الخوارزميات عام ١٩٨٩ بخوارزمية **MD2**، ثم تلتها خوارزمية **MD4** عام ١٩٩٠، ثم خوارزمية **MD5** عام ١٩٩١.

أكثر هذه الخوارزميات أماناً هي **MD5**؛ وهي تستند أساساً إلى خوارزمية **MD4** مُضافاً إليها بعض خصائص الأمان الأكثر إحكاماً.

- **Netiquette** آداب الشبكات

الالتزام بقواعد سلوك وآداب ملائمة عند إستخدام الشبكة

- **NETBIOS** نظام شبكة المدخلات والمخرجات الاساسي

Network Basic Input/Output System يسمح للأجهزة التي تعمل بنظام **DOS** من التحدث مع واستعمال خدمات الشبكة. نفس الاسم هو اسم بروتوكول شبكة محلية يستخدم بشكل واسع في منتجات ميكروسوفت .

- **Newsgroup** مجموعة اخبار

مجموعات الأخبار التي قد يصل عددها الى ٢٠,٠٠٠ مجموعة تكون معاً الـ**Usenet**، وهي بمثابة الصحف التي تناقش جميع موضوعات الحياة وأي موضوع قد يخطر ببالك، ومعظم موفري الخدمة يوجد لديهم موفر مجموعات أخبار **Newsgroup Server**

- On-Line/Off-Line متصل/غير متصل

On-Line تعني أن الكمبيوتر متصل حالياً بالشبكة وعكسه Off-Line أي غير متصل .

- PING مجمع كتلة الانترنت

Packet Internet Grouperبرنامج يستخدم لاختبار القدرة الوصولية وذلك بارسال طلب صدى ICMP إليها وانتظار الرد

- PPP بروتوكول نقطة الى نقطة

Point-to-Point Protocol إحدى وسيلتين لتبادل كتل البيانات عبر انترنت بواسطة خطوط الهاتف (الوسيلة الأخرى هي SLIP) بروتوكول PPP يوفر وسيلة ضغط للبيانات وتصحيح الأخطاء ولايزال تحت التطوير .

- POP بروتوكول مكتب البريد

Post Office Protocol يسمح للمستخدم بتخزين رسائله في كمبيوتر شركة توفير الخدمة كي يقوم باسترجاعها فيما بعد، وهناك ثلاث طبعات لهذا النظام POP و POP2 و POP3.

- Port ميناء (منفذ)

تحديد موقع برنامج معين على كمبيوتر مضيف على الانترنت.. قبل سنوات قليلة كان على المستخدم تحديد البورت بنفسه؛ المنفذ ٢٣ خاص بالــ **Telnet** والمنفذ ٢١ خاص بالــ**FTP**، أما اليوم فمعظم البرامج تحدد البورت أتوماتيكياً .

– Proxy تفويض

طريقة يقوم بمقتضاها جهاز – موجه غالباً – بالرد على طلبات للدخول على مواقع معينة وبذلك يقوم بتنفيذ هذا الطلب بناء على الأوامر التي تلقاها وعلى التوجيه الذي صُمِمَ عليه .

- Queue صف

كتل إحتياطية تنتظر المعالجة

- RAM ذاكرة الدخول العشوائي

Random - Access Memory الجزء من ذاكرة الكمبيوتر الذي يقوم بتخزين المعلومات بصفة مؤقتة بينما هي تحت الاستخدام. أغلب أجهزة الكمبيوتر تحتوي على ٥١٢ كيلوبايت من ذاكرة الرام، هذه المعلومات اذا أغلقت الجهاز ولم تحفظها تختفي بلا رجعة .

– Remote بعيد

لايمكن ربطه مباشرة باستخدام أسلاك محلية ولكنه يحتاج الى أدوات اتصال

أخرى wireless .

- Router موجه

نظام كمبيوتر يتخذ القرارات الخاصة بتحديد اتجاهات الحركة على الانترنت وهو ما يستخدمه أصحاب مقاهى الإنترنت لتوصيل أكثر من جهاز بالإنترنت .

- SLIP بروتوكول الانترنت ذو الخط المتسلسل

Serial Line Internet Protocol هو بروتوكول يستخدم لتشغيل بروتوكول الانترنت **IP** على خطوط متسلسلة **Serial Lines** كدوائر الهاتف. عادة عند الارتباط بموفر خدمة يستخدم اما **PPP** أو **SLIP.**

- Server خادم (موفر)

جهاز يفتح للمستخدمين لتوفير الخدمات لهم كنقل الملفات وغيرها ..
الشخص الذي يدخل على الـ **Server** يسمى **Client**

- Shell المحارة

برنامج يوفر للمستخدم القدرة على التفاعل مع الكمبيوتر .

- SMTP بروتوكول نقل البريد البسيط

بروتوكول يستخدم لنقل البريد الاليكتروني بين الأجهزة .

- Spamming التعميم

مصطلح يطلق على عملية تعميم رسالة في مجموعات الأخبار أو البريد الاليكتروني وهى فى الغالب رسائل غير مرغوب فيها ويقول عنها البعض أنها رسائل الغرض منها النصب أو الإعلان. ويقابله التطهير **Flaming**

- **Standard** معيار (افتراضي)

مجموعة من المواصفات لتصميم البرامج يتم الاعتراف بها من قبل بائعين أو منظمة رسمية دولية .

-Digital Signature التوقيع الرقمي

يُستَخدَم التوقيع الرقمي للتأكد من أن الرسالة قد جاءت من مصدرها دون تعرضها لأي تغيير أثناء عملية النقل. ويمكن للمرسِل استخدام المفتاح الخاص لتوقيع الوثيقة إلكترونياً. أما في طرف المستقبِل، فيتم التحقّق من صحة التوقيع عن طريق استخدام المفتاح العام المناسب.

- SSL بروتوكول الطبقات الآمنة

هو إختصار لـ Secure Sockets Layer وهذا البروتوكول هو المسؤول عن إدارة أمن الإنترنت

T1-

مصطلح **AT&T** يعبر عن وسائل النقل الرقمية **Digital** التي تستخدم لنقل **DS-1** الاشارات الرقمية المشكلة وذلك بسرعة ١,٥ **MB** في الثانية سرعة خارقة وذلك باستخدام خط مؤجر **Leased Line** وهناك أيضاً **T3** التي تستخدم لنقل **DS-3** بسرعة ٤٤,٧٤٦ **MB** في الثانية .

- TCP بروتوكول التحكم بالنقل

يقوم هذا البروتوكول بتمرير المعلومات الى بروتوكول الانترنت **IP** وهو مسئول عن التأكد من وصول الرسالة وأنها مفهومة .

- Telenet الاتصال عن بعد

Telnet هي بروتوكول إنترنت معياري لخدمات الربط عن بعد ويسمح للمستخدم بربط جهازه على كمبيوتر مضيف جاعلاً جهازه وكأنه جزء من ذلك الكمبيوتر البعيد .

فإن كنت من هواة الإبحار في آفاق الويب بحثاً عن مواقع جديدة ومثيرة ف العديد من محركات البحث، ولكن إن كنت من هواة المطالعة وتقصد في بحثك المكتبات العامة ومكتبات الجامعات، فإنك ستُفاجأ عند محاولة النفاذ إلى مثل هذه المواقع على الويب برسالة مفادها: "لا يُمكنك الدخول **(Access is denied)**"، وربما يظن الباحث أنّ هناك خطأً ما في الإنترنت ولكن الحقيقة مغايرة لهذه النتيجة، إذ إن النفاذ إلى هذه المواقع

يحتاج إلى خدمة أخرى من خدمات الإنترنــت، تُــدعى خدمــة تلنــت (Telnet)، تُحقق ما عجــزت عــن تحقيقــه مُستعرضــات الويــب (Web browsers) ، وقد ظهرت هذه الخدمة في أوائل السبعينات مع بداية مسيرة تطور الإنترنت، وقد وفرت كماً كبيراً من المعلومات الــتي لا يُمكن الوصول إليها عادةً على شبكة الويب العالمية.

- Trojan horse حصان طروادة

برنامج كمبيوتر يحمل داخله وسائل تسمح بالدخول الى النظام الذي زُرِعَ فيه .

- URL معين المصادر المنتظم

Uniform Resource Locatorوسيلة معيارية للإشارة للمصادر تقوم بتحديد نو ع الخدمة بالإضافة إلى موقع الملف أو الدليل .

- Unix نظام يونيكس

نظام تشغيل تستخدمه معظم شركات توفير الخدمة ويقوم بربط عدة أجهزة تابعة Clients به للدخول عليه .

- Usenet شبكة المستخدم

شبكة من مجموعات الأخبار تتكون من ١٦,٠٠٠ مجموعة أخبار تهتم بجميع شؤون الحياة .

- Virus فيروس

برنامج يكرر ويضاعف نفسه عن طريق دمج نفسه بالبرامج الأخرى ويضر الكمبيوتر وملفاته المخزنة بداخله .

- White Pages الصفحات البيضاء

مراكز معلومات توفر خدمات ومعلومات عن أشخاص معينين تماماً مثال دلائل يلو بيدجز .

Whois-

برنامج يتيح لمستخدمه البحث في مراكز المعلومات عن أشخاص وعناوين وهو أيضاً موقع هام **www.whois.com** لمعرفة من صاحب موقع ما بشبكة الإنترنت وتاريخ إشتراكه وإنتهاء صلاحيته ومن السيرفر المضيف وكلمات البحث المدرجة بالموقع ، فمثلاً إن أردت معرفة من هو صاحب موقع **www.books4internet.com** فعليك الذهاب إلى موقع **whois** وإدخال الموقع ستجد تاريخ هذا الموقع .

WAIS-

نظام يتيح لمستخدمه البحث عن موضوع معين باستخدام كلمات إفتاحية **Keywords.**

- WWW الشبكة العنكبوتية العالمية

برنامج يعمل باستخدام نقاط ربط **Hypertext link** كي يتمكن

المستخدم من التصفح بواسطة النقر على الروابط .

- Worm دودة

برنامج يكرر نفسه ولكنه يتكاثر في الشبكة بشكل مقصود بعكس الفيروسات، دود الانترنت الذي حدث عام ١٩٨٨ ربما يكون الأشهر فقد استطاع الدود أن يتكاثر في أكثر من ٦٠٠٠ نظام .

– WYSIWYG ماتراه هو ماتحصل عليه

What You See Is What You Get هومصطلح يطلق على بعض برامج تصميم صفحات الويب التي تتيح رؤية ماستكون الصفحة عليه من خلال البرنامج نفسه مثال برنامج فرونت بيدج .

Z – Modem- و Y – Modem و X – Modem-

بروتوكولات تستخدم لنقل الملفات بين حاسبين عادة بواسطة مودم .

- Zone نطاق

مجموعة من أدوات الشبكة **Apple Talk**

Zip code –

الرقم البريدى **Postal code** وهو عبارة عن خمسة أرقام تميز كل منطقة أو حى حتى يتم العثور على العنوان بسهولة.

الفصل الثانى

أمن المعلومات

لقد أعجبنى كثيراً مقالاً بموقع القانون العربى يّعرف أمن المعلومات من :

منظور اكاديمي :

هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها .

ومن منظور تقني :

هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .

ومن منظور قانوني :

فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم

الكمبيوتر والإنترنت) .

واستخدام اصطلاح أمن المعلومات **Information Security** وإن كان استخداماً قديماً سابقاً لولادة وسائل تكنولوجيا المعلومات ، إلا أنه وجد استخدامه الشائع بل والفعلي ، في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال ، اذ مع شيوع الوسائل التقنية لمعالجة وتخزين البيانات وتداولها والتفاعل معها عبر شبكات المعلومات- وتحديداً الإنترنت – إحتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة ، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات ، لدرجة أن كل جهاز أمن بكل دولة الآن أنشأت قسم خاص لمكافحة الإجرام عبر الإنترنت حتى تساعد على تقليل هذه الجرائم بل والتخلص منها إن أمكن.

ولأن الإنترنت تضم مجموعة كبيرة من الشبكات حول العالم وبالطبع لها فوائد كثيرة ، وأصبحت وسيلة سهلة وممتعة تُتيح لملايين البشر الحصول على كم هائل من المعلومات، إضافةً إلى التواصُل وتبادُل المعلومات والرسائل فيما بينهم. ولكن بعض العوامل (مثل الطبيعة المفتوحة لهذه الشبكة، وعدم وجود أي جهة يمكنها الادعاء بأنها تمتلكها أو تسيطر عليها، وعدم وجود قوانين مركزية رادعة)- أدَّت إلى انتشار العديد من الجرائم على الشبكة) مثل: التجسس على حُزَم الرسائل

(packet sniffing)، وكذلك تخريب أجهزة الكمبيوتر وملفاتها (computer hacking)، وَشَنّ هجوم الفيروسات على البريد الإلكتروني، إضافة إلى عمليات الخداع (hoaxes) وغيرها. ورغم أن الإنترنت ليست البيئة الوحيدة التي تحدُث فيها الجرائم والمخالفات القانونية، إذ إن الجريمة ظاهرة موجودة في مجتمعات عديدة، فإن المشكلة الرئيسة تكمن في عدم وجود قوانين دائمة ورادعة تحمي مستخدمي الإنترنت. ومما سبق نجد أن أمن الإنترنت أصبح شأناً مهماً لا بد من حل مشاكله، نظرا لأهمية هذا الأمن في عمليات تبادُل المعلومات الشخصية ومعلومات العمل.

وتشكل قضايا الأمن والتهديدات الناتجة عنها العائق الأكبر أمام اكتساب ثقة الناس ومشاركتهم في تقدم الإنترنت من حيث حركات البيع والشراء عبر شبكة الإنترنت وإجراء الحركات المالية عبرها. وتبقى مسألة الحفاظ على أمن الإنترنت باعتماد وسائل سهلة واقتصادية من أكثر المسائل التي تشكّل حالياً تحدياً كبيراً لهذه التقنية.

لذلك فإن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات – سواء من الناحية التقنية او الأدائية – وكذا هدف التدابير التشريعية في هذا الحقل ، و هدف جميع مستخدمي الإنترنت في

الحصول على المعلومات ونقلها بشكل آمن ، ولضمان نقلٍ آمن للمعلومات بين الأطراف المتصلة ، لابد من ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها :-

- السرية أو الموثوقية **CONFIDENTIALITY**: وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- التكاملية وسلامة المحتوى **INTEGRITY** : التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع .
- إستمرارية توفر المعلومات أو الخدمة **AVAILABILITY** :- التأكد من إستمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وإن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها .

- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به **Non-**

repudiation :- ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف ، بحيث تتوفر قدرة إثبات أن تصرفاً ما قد تم من شخص ما في وقت معين .

وقد تم وضع عناصر ثلاثة بنفس الكيفية مع إختلاف المسميات وهى:

- الخصوصية (privacy)،
- وسلامة المعلومات (Integrity)،
- والتحقق من هوية الأطراف الأخرى (peer authentication)

الخصوصية (privacy)

كي تتم المحافظة على خصوصية الرسالة الإلكترونية، يجب ألا يتمكّن من الاطلاع عليها إلا الأطراف المعنية المسموح لها بذلك. وللحفاظ على الخصوصية، لا بُدَّ من التحكم بعملية الدخول، وأكثر طرق التحكم انتشاراً هي: استخدام كلمات المرور (passwords)، والجدار الناري (firewall)، إضافة إلى شهادات الترخيص (authorization certificates) مثال BBB الأمريكية.

و BBB ترمز إلى **Business better bureau** وهي هيئة أمريكية ، إذا حصل أى صاحب موقع تجارى على هذه الشهادة سيجنى من المال الكثير وذلك لأن هذه الشهادة بمقتضاها يدخل المشترى أو الزبون **customer** وهو متأكد ١٠٠% أنه لن ينصب عليه وذلك لوجود شهادة الـ **BBB** ، وتجد هذه الشهادة بنهاية الموقع .. وطبعاً للحصول هلى هذه الشهادة لابد من توفر شروط أمنية **security** وآمنة **safe** لصاحب الموقع وهذه الشهادة مثل شهادة الأيزو **ISO** التى تجعل المستوردين يشتروون من المصنع الحاصلعلى هذه الشهادة بكل إطمئنان ..

أذكر أن أحد أصدقائى فى نيوجرسى يمكلك موقع مزاد ولكن كان فى بدايته ، فكان الأمر شاق عليه لكى يبيع وينافس أصحاب مواقع المزادات الأخرى ، فاجتهد وحارب حتى حصل على شهادة **BBB** التى كانت بداية طيبة له حيث زادت وشجعت العملاء للشراء والبيع من خلال موقعه ..

سلامة المعلومات (Integrity)

لا بُدَّ من حماية عمليتي نقل المعلومات وتخزينها، وذلك لمنع أي تغيير للمحتوى بشكل متعمَّد أو غير مُتعمَّد. وتكمن أهمية ذلك في الحفاظ

على محتوى مفيد وموثوق به. وفي الغالب، تكون الأخطاء البشرية وعمليات العبث المقصود هي السبب في تلف أو تشويه البيانات. وينتج عن ذلك أن تصبح البيانات عديمة الجدوى، وغير آمنة للاستخدام.

ولتلافي تشويه أو تلف البيانات، يُمكن استخدام تقنيات مثل: البصمة الإلكترونية للرسالة (**message digest**) والتشفير (**encryption**)، ومن المفيد أيضاً استخدام برمجيات مضادة للفيروسات (**anti-virus software**) لحماية أجهزة التخزين من انتهاكات الفيروسات التي تتسبب في تلف أو تشويه البيانات. ومن المهم أيضاً الاحتفاظ بِنُسَخ احتياطية (**backup**) لاسترداد البيانات المفقودة في حال تعرضها للضرر، أو في حال تعطُّل الشبكة أثناء عملية النقل.

التحقق من هوية الأطراف الأخرى (Peer Authentication)

يجب التأكد من هوية الأطراف المعنية بعملية تبادل البيانات، إذ يجب على كلا الطرفين معرفة هوية الآخر لتجنب أي شكل من أشكال الخداع (مثل عمليات التزوير وانتحال الشخصيات). وهناك بعض الحلول والإجراءات للتحقق من هوية الأطراف المتصلة مثل: كلمات

المـــرور (passwords)، والتواقيـــع الرقميـــة (digital signatures)، والشـــــهادات الرقميـــــة (digital certificates) التي يُصدرها طرف ثالث. ويُمكن أيضـــا تعزيـــز الأمن بالاعتماد على بعض المميزات المحسوسة مثل: بصـــمة الإصـــبع (print finger)، والصوت، إضافة إلى الصورة.

أمن المعلومات في المؤسسات التعليمية

يتعرض العديد من شـــبكات الحاســـب الآلي إلى عمليـــات هجـــوم واختراقات بسبب السطو على المعلومات أو التخريب بمـــا في ذلـــك شبكات المؤسسات التعليمية، وكلما كانت المعلومات هامة وحساســـة كلما زاد اهتمام المخربين والمخترقين بها، مما يستدعي وجـــوب أخـــذ التدابير اللازمة لحماية المعلومات والشبكات، وقد أزداد اهتمام التقنيين بهذا الجانب مع زيادة الهجمات على الشبكات والسطو على المعلومات إلى أن أصبح أمن المعلومات تخصصا منفرد ضمن مجالات الحاسب الآلي، كما أصبح له شركات خاصة تقوم بإنتاج نظم وعتاد الحماية ووضـــع الحلول الشاملة له.

الفصل الثالث

الهاكرز و الكراكرز

البعض منا يعتقد أن كلمة (هاكرز) كلمة سيئة و مضمونها سيئ ، و هذا سببه أن البعض لا يعلم معنى كلمة (هاكرز) و في أغلب الأوقات البعض منا يخلط بين كلمة (هاكرز) و كلمة (كراكرز) ، إذاً علينا أن نعرف **من هم الهاكرز** ، و **من هم الكراكرز** ، و ما الفرق بينهما .

اولاً :من هم الهاكرز ؟

كلمة (الهاكرز) ليست كما يظن كثير من الناس أنهم أنــاس أشــرار يقومون بالتخريب والتدمير والإقتحام المغرض ولكن هي كلمة تحمــل معنى آخر وهو (مبتكر لنظم المعلومات و البرمجيات) فالهاكرز هم على مستوى عالي وتقنى حتى يمكنهم ذلك من فك الشفرات والثغرات التى قد بل بالفعل تؤذى كثير من الهيئات والشبكات ، و هي أيضاً عبــارة عن إسم إختاره لأنفسهم مجوعة من المبرمجين الأكفاء المهــرة القــادرين على ابتكار البر مج و القادرين أيضاً على حل مشــكلات الــبرامج في الحاسب الآلي في جميع أنظمته و التعامل مع جميع شبكات الحاسب الآلي و يتقنون على الأقل أربع لغات من لغات البرمجة المعروفة ، و هذا ممــا يجعلهم يستطيعون إكتشاف الثغرات و الأخطاء في الأنظمة و الشبكات

و العمل على تلاشيها و تصحيحها ، فـ (الهاكرز) هم الذين صنعوا أغلب برامج الحاسبات و الشبكات و البرمجيات ، و الدلالة على ذلك أنه يجب أن نعلم أن أشهر (الهاكرز) حتى الآن هو (تيـــور فالـــدس لينوس) أحد أهم متطورين نظـــام التشـــغيل (Unix) أول نظـــام حاسبات عرفه العالم سنة (١٩٧١) تقريباً ، و هو أيضاً المبتكر لنظام التشغيل الأكثر أماناً و تطوراً و شهرة في العالم و هو نظام التشـــغيل (Linux) ، و قد بدأ ظهور (الهاكرز) أثناء الحرب العالمية الثانية و كانوا في هذا الوقت يعملون مع الجيوش لفك شفرات إشارات الأجهزة اللاسلكية للجيوش الأخرى بدقة و سرعة كبيرة جداً ، ثم بعد ذلـــك أنتشر (الهاكرز) أو المبرمجين بعد إنتهاء الحرب العالمية الثانية ، و عنـــد إختراع أول جهاز حاسب آلي ، كان لابد له من نظام تشغيل و من هنا بدأ دور الهاكرز في الظهور و البرمجة و الإبتكار .

ثانياً :من هم الكراكرز ؟

كلمة (كراكر) & (Cracker) هي كلمة بالإنجليزيـــة تعـــنى (الكسر أو التكسير) و معناها العام بالنسبة لموضوعنا أن (الكراكرز) كلمة تعني التخريب والعبث و التحطيم ، و هي عبارة عن إسم إختاره لأنفسهم مجوعة من المخربين المهرة القادرين على إختراق أي شـــبكة أو أي جهاز حاسب ، و لكن يجب أن نعلم أن إختراق المواقع الإسرائيلية

و الشبكات الإسرائيلية التى تقدم مواقع إباحية وجنسية و جميع أنــواع البريد الإليكتروني الإسرائيلي **spam e-mail** من قبل العــرب و المسلمين لا يعتبر هذا كراكر لأنه يستهدف دولة معينة أو فئة معينة ، و إنما يعتبر هذا أمر واجب علينا جميعاً ، لأن هذا جهاد و حرب ، و حتى نحاول بقدر المستطاع أن نطهر كل أماكن ومواقع الإنترنت من كـــل أفاعيل أعداء الله و حتى يتعظوا و يعلموا أننا قوة لا يستهان بهـــا عنـــد اتحادها ، **فالكراكرز** لا يقلون مهارة ولا كفاءة عـــن (الهـــاكرز) ، و لكنهم على العكس تماماً يستخدمون هذه المهارة في التخريب و السرقة و الحصول على الأموال بطريقة غير مشروعة ، و لعلنا نذكر أن مـــن أشهر (الهاكرز) في العالم (كيفن ميتنيك) الذي أصبح أســـطورة في الكراكرز و أصبح هو مثلهم الأعلى ، نظراً لموهبته و قدرته الفائقـــة في السرقة و تدمير الأجهزة و الشبكات و المواقع بشكل عـــام ، و قـــد أصبح (كيفن ميتنيك) أشهر (كراكرز) بعدما نفذ أكبر عملية سرقة تاريخية إليكترونية عرفها العالم ، حيث قام بسرقة حـــوالي أكثـــر مـــن ٢٠٠٠٠٠ أو مائتان ألف رقم لبطاقات إئتمان ســـنة (١٩٩٥) ، و قد بدأ ظهور (**الكراكرز**) تقريباً بعد الحرب العالمية الثانية في حين كان (الهاكرز) يعملون مع الجيوش ، كانوا هم مختبئين و يخططون و يدبرون لعملياتهم اللصوصية و كانت أهم اهتماماتهم في ذلك الوقت التصـــنت والتجسس على التليفونات والأجهزة اللاسلكية وكـــان هـــذا في أول

الأمر على سبيل المتعة وهذا باختصار كل شيء عن (الكراكرز).

مـــــاهو الفـــــرق بـــــين الهـــــاكر والكراكـــــر؟

في الحقيقة مما سبق يتضح لنا أن الفارق هو فارق أخلاقي وليس فارق علمي.

الهاكر : هو الشخص الذي يعرف عدة لغات معرفة جيدة بحيث يكون لــه القدره على كتابه برامج مفيده و مبتكره

إذاً فالهاكر يخترع ويبتكر .

الكراكر : هو الشخص الذي يحاول بطرق غير شرعيه أن يدخل أو يدمر الأمن للنظام أو الشبكه بنية خبيثه

و الكراكر يخرب ويسرق

و بعض الأحيان يطلقون عليهم هاكر ذو القبعه السوداء

(Black hat hacker)

أما الشخص الذي يحاول أن يدخل على النظام أو الشبكه بغرض مساعدة صاحب النظام بأن يحذره بأن هناك عيوب في أمن النظام فيطلق عليهم هاكر ذو القبعه البيضاء

(White hat hacker)

الفصل الرابع

أنواع الهجوم والإختراق Types of Attack

١. التصنت على الرسائل Interception Attacks:

فى هذه الحالة يقوم المهاجم بمراقبة الإتصال بـين المرسـل والمسـتقبل للحصول على المعلومات السرية وهو ما يسمى بالتصنت على الإتصال (**Eavesdropping**).

٢. هجوم للإيقاف Interruption Attacks:

وهذا النوع يعتمد على قطع قناة الاتصال لإيقاف الرسالة أو البيانـات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض الخدمة (**Denial of service**).

٣. تعديل محتوى الرسالة Modification Attacks:

وهنا يتدخل المهاجم بين المرسل والمستقبل (يعتبر وسيط بين المرسل والمستقبل) وعندما تصل إلى الـ**Attacker** فإنه يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل ، والمستقبل طبعاً لا يعلم بتعديل الرسالة من قبل الـ**Attacker** فيقوم بإعطاء معلومات سرية إلى

المهاجم.

٤. الرسائل المزورة Fabrication Attacks:

وهنا يرسل المهاجم رسالة مفادها أنه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة مثلاً .

واعلم أن أسهل طرق الإختراق هي :

١. عن طريق المتصفح الإكسبلورر إذا لم تتم ترقيته بإستمرار حيث يستطيع الهاكر دخول جهازك عن طريق متصفحك بواسطة سكربت معين ومعروف بين أوساط الهاكرز والمبرمجين.

٢. عن طريق البريد الإليكتروني عند إرسال مرفقات تروجان أوفيروسات مع البريد.

٣. عن طريق إستعمال برامج المحادثه مثل الماسنجر و **ICQ** و **MIRC** وهذه البرامج يستخدمها كثير من الضحايا.

٤. عدم ضبط إعدادات المتصفح حتى يمنع دخول الكوكيز الغير آمنه إلى الجهاز.

٥. عدم ترقية نظام الويندوز المستخدم بإنتظام حيث يتم إكتشاف ثغرات أمنيه في النظام من قبل شركة مايكروسوفت.

٦. تنزيل البرامج بإستمرار دون التأكد من نظافتها من التروجان والفيروسات والكارثه عند البحث عن الكراك لتلك البرامج في مواقع الهاكرز الملغمه بالإسكربت الذي يخترق المتصفح والدخول لجهاز الضحيه.

٧. عدم وجود برامج حمايه يتم ترقيتها بإستمرار.

الإجراءات المضادة للتهديد Threats أو الهجوم:Attacks

- وضع جدران نارية **Firewalls**
- برامج مكافحة الفيروسات **Anti-virus software**
- التحكم بالدخول **Access Control**
- مضاعفة أنظمة التحقق من المستخدم **Two-factor authentication systems.**
- التدريب الجيد للموظفين **Well-trained employees**

قال تعالى: ولا تجسسوا ، ولا يغتب بعضكم بعضا .. الآية ١٢ الحجرات

و إعلم اخى العزيز أن العلم امانة وستسأل عنه يوم القيامة ،

قال تعالى: *" إنا عرضنا* **الأمانة** *على السماوات والأرض والجبال فأبين أن يحملنها واشفقن منها وحملها الإنسان إنه كان ظلوما جهولا* " الأحزاب آية ٧٢

فلا تغتر بعلمك وتستخدم هذه الأمانة فى أذى الناس ، كن متواضعاً واعلم أن الله سبحانه وتعالى قادر ان يسلب منك هذا العلم ويعطيه لغيرك ليفيد به الناس .

واعلم ان ديننا الحنيف حذر بعدم الإضرار بالناس إن كان في ارزاقهم او فى علمهم أو فى أنشطتهم ولا تكن من ذوى النفوس الضعيفة فهم جاهلون بأن الله هو الرقيب وإنه سبحانه وتعالى ليس بظلام للعبيد .

فيمكنك أن تكون هاكر بل وكراكر ولكن فى سبيل الله ، ما بالك إذا إستخدمت كل ما لديك من علم و فنون وتقنية فى غلق المواقع الإباحية وتتبع أسرار العدو وصد الهجوم والإختراقات من قبل العدو

اليس ذلك فى سبيل الله.

الفصل الخامس

التخلص من الفيروسات وملفات التجسس

الفيروس

هو برنامج صغير غالباً يكون غير مرئى يربط نفسه ببرنامج آخر ليتمكن من التكاثر و التكرار و الانتشار من خلال هذا البرنامج فعند تنفيذ هذا البرنامج المصاب بالفيروس ينتقل الفيروس إلى الذاكرة للجهاز المرسل إليه الفيروس و يستقر فيها و يصيب كل برنامج يتم تحميله فى الذاكرة بعد ذلك قبل إعادة تحميله و قد ينشط الفيروس فى يوم معين كما حدث مع فيروس تشرنوبل فى ٢٤ أبريل أو عند نسخ برنامج معين أو عند تنفيذ برنامج عدد من المرات أو بعد عدة مرات من إعادة التحميل و هناك فيروسات تصيب الملفات و أخرى تصيب الجزء الخاص بتحميل الجهاز و الموجود فى الاسطوانة الصلبة أو الاسطوانة المرنة.

قد يؤدى الاصابة بالفيروس الى تعطيل عمل البرامج او تقليل سرعته او اصابة الجزء الخاص بتشغيل جهاز الكمبيوتر مما يؤدى الى ايقاف عمل الجهاز او قد يؤدى الفيروس الى مسح منطقة جدول التقسيم. جدول التقسيم هو فهرس يحتوى على اسماء الملفات و اماكن وجودها على القرص الصلب .

تستهدف الفيروسات:

١- البرامج التنفيذية مثل:

.com, .exe, .ovl, .drv, .sys, .bin, .vbx,.dll

٢- البرامج التحميلية مثل:

Boot Record, Master Boot, FAT, PartitionTable

٣- متعددة الأهداف (البرامج التنفيذية والتحميلية)

كيف يمكن اكتشاف وجود فيروس على الحاسب الشخصي

تواترت في الآونة الأخيرة تحذيرات كثيرة بشأن إنتشار فيروسات الحاسب بحيث صار من السهل أن ينسب المرء أي إضطراب مريب يطرأ على أداء حاسبه الشخصي إلى إحتمال إصابته بفيروس. ولكن الفيروسات في حقيقة الأمر لا تكون مسئولة في بعض الأحيان عن أي إضطراب أداء الكمبيوتر، حيث إن بعض هذه المشكلات يكون ناجماً عن أسباب أخرى.

وربما يفاجأ المستخدم عند فتح مستعرض الإنترنت بوجود موقع إباحي على شاشة الكمبيوتر بدلاً من صفحة البدء الأصلية ويفترض أن

السبب في ذلك هو وجود فيروس ولكنه لا يكتشف وجود أي مشكلة عند تشغيل برنامج مكافحة الفيروسات ويتساءل عما إذا كان السبب في هذه المشكلة هو وجود فيروس.

ويرجح أن يكون السبب وراء هذه المشكلة هو قيام موقع من المواقع التي زارها المستخدم "بخطف" مستعرض الإنترنت الخاص بالحاسب. فأحيانا ما يتلقى المستخدم رسائل بريد إليكتروني تحتوي على عناوين مواقع إليكترونية تبدو مشروعة، ولكن هذه المواقع في حقيقة الأمر تدخل تعديلات على مواصفات صفحة البدء.

وأحيانا ما يتلقى المستخدم رسائل تحذيرية بشأن تغيير مواصفات الصفحة ولكنه لا يعرف في بعض الأوقات كيفية التعامل مع هذه التحذيرات ويبادر بالضغط على مفتاح الموافقة. ولا تمثل هذه التغيرات من الناحية الفنية فيروسات ولكنها بلا شك تثير إزعاج المستخدم.

ويتعين من أجل استرجاع المواصفات الأصلية لصفحة البدء فتح مستعرض الإنترنت وإختيار قائمة أدوات ومنها إلى قائمة خيارات الإنترنت ثم يتوجب إلغاء عنوان الموقع الاباحي المدون في الخانة المخصصة لتسجيل عنوان موقع البدء وكتابة إسم صفحة البدء الأصلية. وعادة ما تتسبب الفيروسات في بطء عمل الحاسب وعملية تحميل البرامج واختفاء بعض الملفات المسجلة على الكمبيوتر والحيلولة دون عمل البرامج بشكل منتظم أو منع عملها على الاطلاق.

ومن الضروري أن يعرف المستخدم أن هناك عوامل أخرى خلاف الفيروسات يمكن أن تكون سبباً في إضطراب أداء الكمبيوتر. ولهذا السبب تكمن الصعوبة في تحديد ما إذا كان الجهاز مصاباً بفيروس أم لا. تماماً حينما يختلف كثير من الأطباء فى تشخيص مرض واحد للأسف . وأفضل الحلول لمعرفة ذلك تتمثل في إستخدام نسخة مطورة من برنامج خاص بمكافحة الفيروسات من إنتاج شركة معروفة. وتستخدم بعض الفيروسات قائمة عناوين البريد الاليكتروني كي ترسل نفسها في صورة ملفات ملحقة إلى أجهزة كمبيوتر أخرى. ولهذا السبب يتعين على المستخدم الإحتفاظ بنسخة متطورة من برامج مكافحة الفيروسات ويقوم بتشغيلها بحيث تتولى فحص الرسائل الإليكترونية الواردة والصادرة بصورة تلقائية ومنع انتقال الملفات المصابة بفيروسات.

ويتعين على المستخدم عندما يتشكك في وجود فيروس بأحد الملفات على جهاز الكمبيوتر الخاص به أن يبادر بإرسال هذا الملف إلى أحد مختبرات فحص الفيروسات المنتشرة في مختلف أنحاء العالم ولها مواقع عديدة على شبكة الانترنت.

اولاً : التخلص من الفيروسات :

يمكن الوقاية من الفيروس بتشغيل إحدى برامج الـــ **anti virus** التى تعمل فى بيئة **Windows**

و التى تظل موجودة فى ذاكرة الحاسب و عند دخول الفـيروس بـأى طريقة فإنها تمنعه و ترسل رسالة تحذيرية لمستخدم الحاسب مثل برنامج **Norton Anti Virus**

هذا البرنامج يقوم بفحص الذاكرة و ملفات النظام و قطاعات التشغيل عند بدء تشغيل الجهاز به و يمكنك إستخدامه للبحث عن الفيروسات و إزالتها سواء كان على القرص الصلب أو المرن و يمكنـك إسـتخدامه لفحص أى ديسك مرن قبل إستخدامه و هو لديـه قائمـة بهـا آلاف الفيروسات يقوم بالبحث عنها و إزالتها لاحظ كذلك أنه يجب تطـوير **update** برامج الوقاية و الكشف عن الفيروسات باسـتمرار حـتى تواكب ظهور الأنواع الجديدة من الفيروسات.

وإختيار برنامج الحماية "مضاد الفيروسات" الأنسب لـك ولجهـازك كما نعلم ، هناك العديد من البرامج التي يقول مبرمجوهـا أنها هـي الأفضل و تستطيع القضاء على كل الفيروسات و حـتى الفيروسـات الغير معروفه .

لا تصدق كل ما يقال .. فقد أثبت التجارب العمليه أن ٩٩% مــن البرامج التي تم تجربها لم تستطع أن تحمي الأجهــزة الــتي تم إصــابتها بفيروسات تتراوح خطورتها بين خفيف الخطــورة إلى خطــير جــداً.

ومن أشهر مضادات الفيروسات **Anti-virus**

Norton anti-virus
PC Cillin
KasperSky Antivirus
McAfee Virus scan
NOD32
Vcatch

التخلص من الفايروسات دون الحاجة الى برامج

سوف يتم الكشف عن الفايروسات من خلال موقع **Symantec** المتخصص في هذا العمل والذي يقدم لنا برامج حماية المختلفة منها برنامج **Norton Antivirus .**

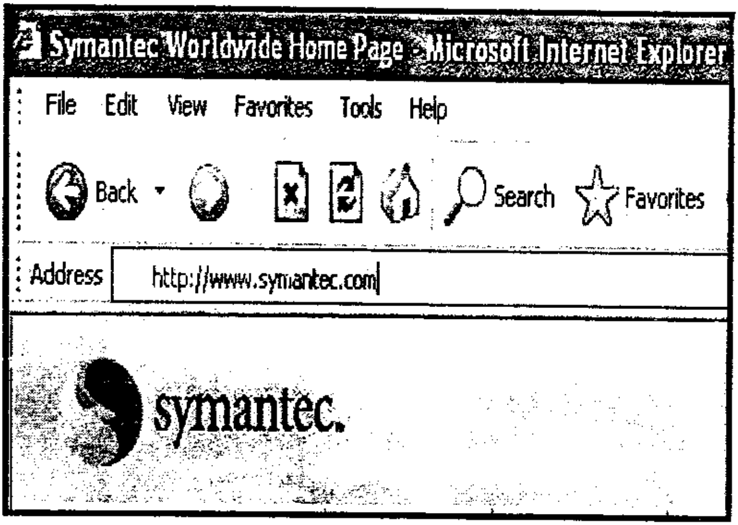
ويقدم لنا ايضا خدمة الكشف والتخلص من الفيروسات عن طريق الانترنت بدون حاجة الى البرنامج في جهازك.

ولكن هذا لا يعني أن تتخلى عن برامج الحماية ولكن هناك بعض الفيروسات التي

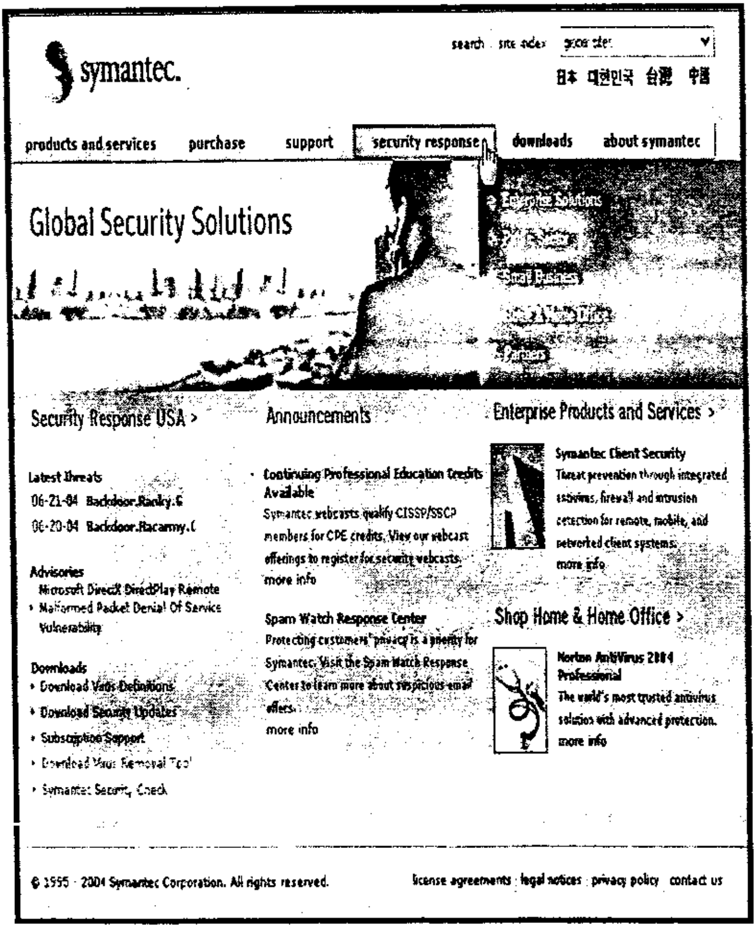
تغلق برامج الحماية ، فهذا واحد من الحلول للتلخص منها.

أولا قم بالدخول الى موقع **Symantec** الموجود على هذا العنوان:

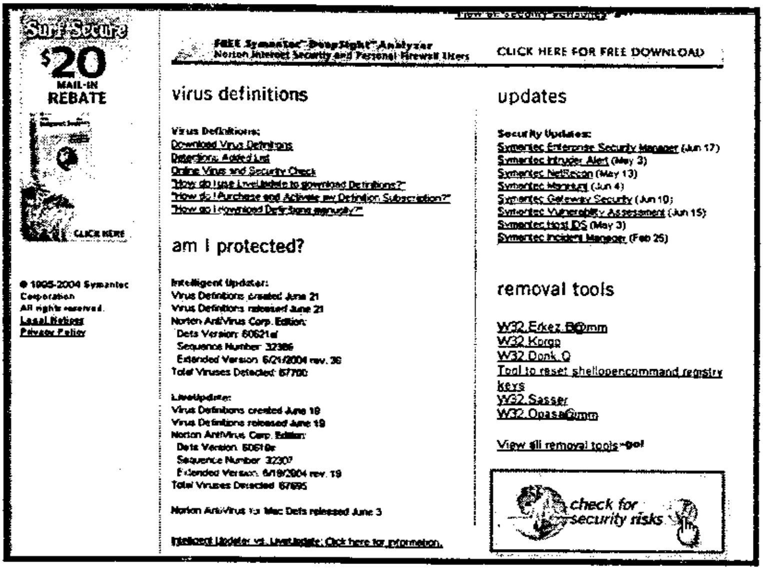
www.Symantec.com



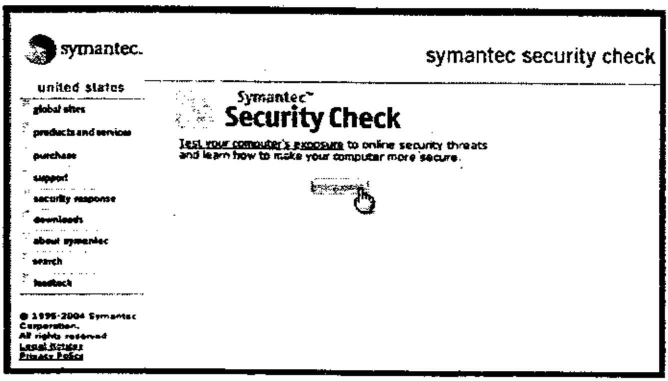
قم بإختيار **security response**



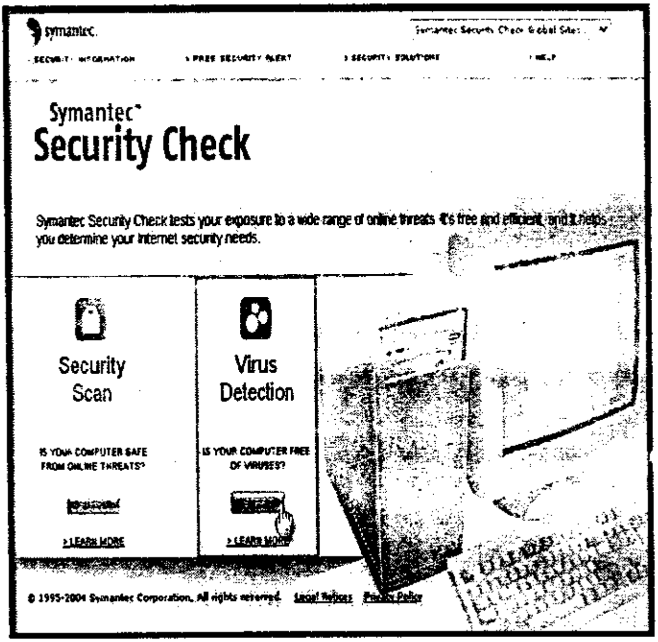
بعد ذلك إبحث عن **check for security risk** وإضغط عليها


Surf Secure
$20
MAIL-IN
REBATE
CLICK HERE
CLICK HERE FOR FREE DOWNLOAD
virus definitions
Virus Definitions:
Download Virus Definitions
Online Virus and Security Check
am I protected?
Intelligent Updater:
Virus Definitions created June 21
Virus Definitions released June 21
Norton AntiVirus Corp. Edition:
Sequence Number 32386
Extended Version 6/21/2004 rev. 36
LiveUpdate:
Virus Definitions created June 19
Virus Definitions released June 19
Norton AntiVirus Corp. Edition:
Extended Version 6/19/2004 rev. 19
Total Viruses Detected 67695
Norton AntiVirus for Mac Defs released June 3
updates
Security Updates:
Symantec Enterprise Security Manager (Jun 17)
Symantec Intruder Alert (May 3)
Symantec NetRecon (May 13)
Symantec Gateway Security (Jun 10)
Symantec Vulnerability Assessment (Jun 15)
Symantec Host IDS (May 3)
Symantec Incident Manager (Feb 25)
removal tools
W32.Erkez.B@mm
W32.Korgo
W32.Donk.Q
Tool to reset shellopencommand registry keys
W32.Sasser
W32.Opaserv@mm
View all removal tools - go!
check for security risks

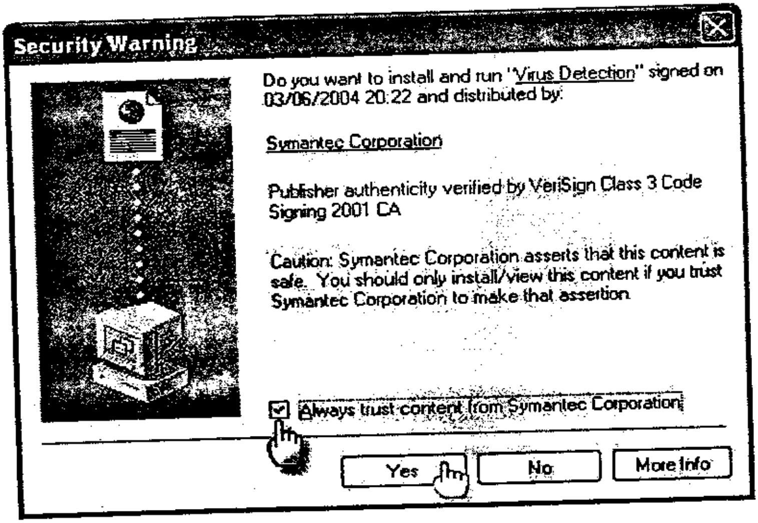
إضغط على **Go**


symantec.
symantec security check
united states
global sites
products and services
purchase
support
security response
downloads
about symantec
search
feedback
© 1995-2004 Symantec Corporation.
All rights reserved
Legal Notices
Privacy Policy
Symantec™
Security Check
Test your computer's exposure to online security threats and learn how to make your computer more secure.

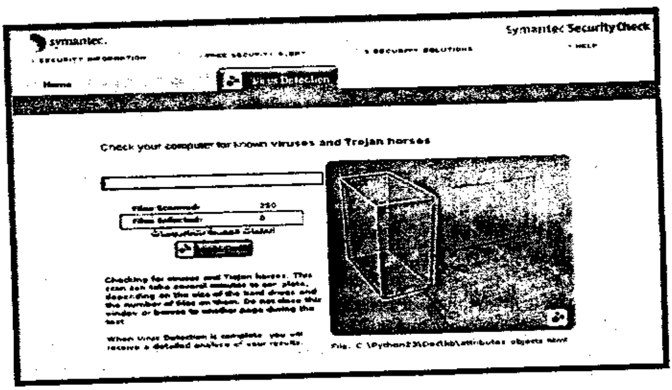
قم بالضغط على **Start** الموجود تحت **Virus Detection**



بعد ذلك سوف تظهر لك رسالة قم بالضبط على المربع لكي يظهر عليه علامة ، واضغط **Yes**



سوف يبدأ الموقع بالبحث في جهازك عن الفيروسات وفي نهاية العمل سوف يظهر تقرير كامل عن حال جهازك ، فحاول أن تجرب هذه الطريقة الآن ..



ثانياً إزالة ملفات التجسس

Remove spy ware

١- إختيار برنامج الحماية "مضاد ملفات التجسس" الأنسب لك و لجهازك لتنظيف جهازك من أى برامج تجسسية ، ويوجد العديد من البرامج التي تقوم بهذه المهمة ومن أهمها **Ad-Aware** و **Spy weeper** ، احرص على تحديث مضاد الفيروسات الخاص بك ، واستخدم برنامجاً غير معروف (غير منتشر) بصورة كبيرة لفحص جهازك من فترة لأخرى - يمكنك تثبيته على جهازك وعدم تشغيله الا في حالة الفحص فقط .

٢- إختيار برنامج الحماية "مضاد الإختراقات أو الحائط الناري أو الجدار النارى الأنسب لك و لجهازك.

معظم البرامج المتخصصه بهذا المجال تفي بالغرض لكن لتعرف كل ما يحدث بجهازك وتمنع أي إتصال بين برامجك (التي قد تكون مضره أو مخله بأمن جهازك) و الإنترنت ، يمكنك إستعمال : **Zone Alarm**

ولنعلم جميعاً أن عملية التجسس قد تكون من مصنعى ومبرمجى برامج النظام والتصفح كما هو الحال فى مايكرو سوفت التى تتجسس علينا

من خلال ويندوز .

٣- المتابعة لتحديثات البرامج التي تستخدمها في موقعك فمثلاً إن كنت تستخدم منتدى في موقعك ، فلابد أن تتابع ولو بشكل شبه يومي لآخر التحديثات التي ظهرت لهذا البرنامج وكذلك سد جميع الثغرات والترقية إلى آخر إصدار.

٤- حماية المجلدات المهمة بجدار ناري من خلال لوحة التحكم الخاصة بموقعك ولو على سبيل المثال **cPanel** فلتقم بحماية المجلدات المهمة مثل المجلد **admin** للمنتدى ، حتى إذا ماتم إختراق الموقع لاقدر الله ، فلن يستطيع المخترق الدخول للوحة التحكم إلا بعد تخمين كلمة السر الثانية

٥- عدم إستخدام التصريح ٧٧٧ إلا عند الضرورة القصوى ويجب عليك أن تقوم بحماية المجلد أيضاً بجدار ناري حتى تضمن عدم وجود تلاعب ، كذلك إن كنت تستخدم برنامج لرفع الملفات فعليك إبطال تحميل الملفات المؤثرة مثل

ملفات **.php .php3 .phtml .pl .cgi** ، وذلك من خلال الملف **htaccess** لحماية موقعك.

٦- لاتعطي صلاحيات الدخول إلى لوحات التحكم في موقعك إلا لشخص تثق فيه ١٠٠ %

ومع كل هذه الإحتياطات لايوجد شئ إسمه حماية ١٠٠% ولكن نسعى لإغلاق كل السبل لتخريب مواقعنا من قبل الكراكرز .

يقول الله تعالى: " ولا تجسسوا ولا يغتب بعضكم بعضا أيحب أحدكم أن يأكل لحم أخيه ميتا فكرهتموه واتقوا الله إن الله تواب رحيم "

سورة الحجرات الآية ١٢

الفصل السادس

الحفاظ على البريد الإليكتروني من الإختراق

١. يجب أن تكون كلمة المرور(كلمة السر) **pass word** طويلة وتحتوى على حروف وأرقام ورموز مثال **sc2004x**

٢. أن تكون كلمة السر عشوائية وغير مرتبة ومسلسلة ،

٣. لا تكتب الأسماء أو تاريخ الميلاد أو أسماء الأولاد أو رقم الهاتف أو المدينة.

٤. لا تكشف عن معلومات خاصة لأى شخص تقوم بمراسلته عبر البريد الإليكترونى

٥. لا تجعل إسم المستخدم **user name** نفسه كلمة المرور أو حتى أن تضيف إليها بعض الحروف أو الأرقام مثال:

User name : khaledmk
Pass word : khaledmk2000

هذا خطأ كبير يسهل على المخترق معرفة كلمة السر خصوصاً أن هناك برامج تقوم بتخمين كلمات السر.

٦. حاول أن تجعل لكل بريد كلمة مرور خاصة به إن كان لك أكثر من بريد إليكترونى

٧. إن كنت سريع النسيان فاكتب كلمة السر فى ورقة أو حتى فى

ملف بجهازك بشرط أن تقوم بعملية تمويه لكلمة المرور ، فمثلاً إن كانت كلمة المرور الخاصة بك هى **egypt2000** مثلاً فاكتبها فى مذكرتك بأن تضف حروف أو أرقام زائدة للتمويه فمثلاً يمكنك كتابتها **kmkegypt2000** أو **egypt2000yes** ، وبالطبع أن فقط تعلم أن هذه الإضافة مجرد تمويه للكلمة الحقيقية وهى **egypt2000** بهذه الطريقة يمكنك حفظ كافة كلمات المرور فى ملف بالإنترنت أو فى ورقة.

٨. أن يكون لك بريد خاص لإستخدامه فى المنتديات والقوائم البريدية و الماسنجر

٩. أن تقوم بتغيير كلمة السر كل فترة للتأكد من أنك فى أمان ممن قد يكونوا بالفعل يستغلون كلمة السر فقط لفتح رسائلك والإطلاع على أسرارك وأعمالك دون أن تدرى.

١٠. لا تدخل لبريدك إلا من موقعه الأصلى حتى لا تقع فى الفخ

١١. عند الإنتهاء من قراءة وتصفح رسائلك إضغط على أيقونة الخروج **log out** أو **exit** لغلق صندوق البريد.

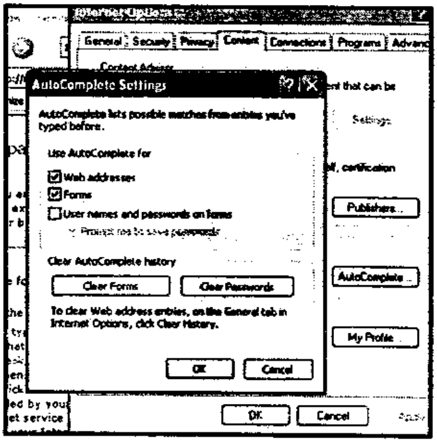
١٢. لا تقوم بفتح ملفات مرفقة تأتى إليك من بريد **e-mail** مجهول وأنصح أن لا تفتح مطلقاً أى بريد لا تعرف مصدره.

١٣. إرسال رسالة فوراً لمدعم خدمة البريد إن كانت مجاناً مثال ياهو بأن بريدك قد سرق .

١٤. حاول أن تقوم بتفريغ صندوق البريد ووضع (حفظ) ملفاتــك ورسائلك الواردة إليك داخل ملف بجهازك ويستحسن فى قــرص مرن أو CD ثم قم بحذف جميع رسائلك من بريدك الإليكتــرونى ، قم بهذه الطريق كل فترة ..

١٥. لا تجعل إسم المرور مخزن(**remember pass word**) فى الجهاز ، أى لا تجعل إسم المرور يأتى إليك تلقائيــاً (الإكمــال التلقائى **auto complete**) بمجرد كتابة إسم المستخدم كما يفعل بعض المستخدمين ، فهذا يعطى فرصة للمخترقين للوصول إلى كلمة السر بسهولة ، ولتعطيل هذه الخاصية إتبع مــا يلــى مــن إكسبلورر :

Tools
Internet options
Content
Auto complete



User names and pass words on forms: (remove the sign)
Press ok

عند دخولك بعد ذلك الموقع لكتابة إسم المستخدم وكلمة السر ستأتى نافذة أو تجدها تحت نافذة كلمة المرور : هل تريد الإكمال التلقائى أو هل تريد حفظ كلمة المرور ، بالطبع إختر لا .

الفصل السابع

تأمين الدفع الإليكترونى

أمن الانترنيت

لقد فرضت شبكة الإنترنت علينا بل و أصبحت أحد مستلزمات الحياة اليومية . فهي توفر وسيلة للدخول إلى كم هائل من المعلومات، وتضعها في حوزتنا بكل سهولة. وأهم من ذلك، أنها باتت تلعب دوراً هاماً في أعظم إبداعات و إختراعات القرن العشرين والواحد وعشرون وهي التجارة الإليكترونية أو **e-Commerce**.

فإلى جانب إمكانية الإنترنيت بوضع كميات غير محدودة من المعلومات بين أيدينا، هناك إمكانية شراء المنتجات والخدمات دون مغادرة المنزل، فالتجارة الإليكترونية تعني كل معاملات البيع والشراء وتبادل المعلومات ، أى أنه بمقدورنا القيام بشراء الكتب، وأجهزة الكمبيوتر، وتذاكر السفر، والسيارات، وغيرها في أي لحظة.

ومع أن هذه الفكرة كانت مشجعة في بادئ الأمر، إلا أن إنتشارها كان بطيئاً نسبياً بسبب مخاوف العامة، فحفظ المعلومات المصرفية وبيانات بطاقات الائتمان في مكان مجهول يعد مخاطرة كبيرة. ومع أن هذا الخطر محدود، إلا أنه لايزال موجوداً.

لهذا الخطر علاقة كبيرة بحقيقة أن معلومات بطاقات الإئتمـان ترسـل ضمن نص غير مشفر، وهذا يعني أنه يمكـن سـرقة هـذه المعطيـات واستخدامها بهدف الإحتيال. لقد تم تطوير تقنيات مختلفة للتغلب على هذه المشكلة وحماية المستهلك، مما زرع الثقة في نفوس الناس وشجعهم على الشراء عبر الإنترنيت.

فكان ظهور بروتوكول ***S-HTTP*** هو نسخة أمنية من بروتوكول **HTTP** ويُستخدم للإتصال مع مواقع الويب. إن أحد مزايا بروتوكول **S-HTTP** هو أنه ليس بروتوكولاً خاصاً، الأمر الذي ساعد على إنتشاره في غالبية برمجيات خادمات الويب، ومع ذلك فإن دعم برامج المتصفحات لهذا البروتوكول لايزال محدوداً.

وقد أنتجت شركة **Netscape** بروتوكولاً منافساً يدعى ***SSL*** وقالت الشركة أنها ستقوم بدعم بروتوكول **S-HTTP** ضمن برامجها في المستقبل القريب.

إذاً بإمكان المستخدمين التعامل مع كلا البروتوكولين، والإتصال بالخادمات التي تستعمل **HTTP** أو **SSL**.

هناك أنواع كثيرة يمكنك منها معرفة إذا كان الموقع الذى تعمل من خلاله أو تحول نقوداً من خلاله آمناً بتلك البروتوكولين أم لا :

المثال الأول : حرف الـــ S بجوار http

هو دليل على أن هذا الموقع محمى ببروتوكول **https**

وحرف **s** يرمز إلى أن الموقع مؤمن **secure**

Secure Hypertext Transfer Protocol،

وهو بروتوكول النقل الآمن لنصوص الانترنت

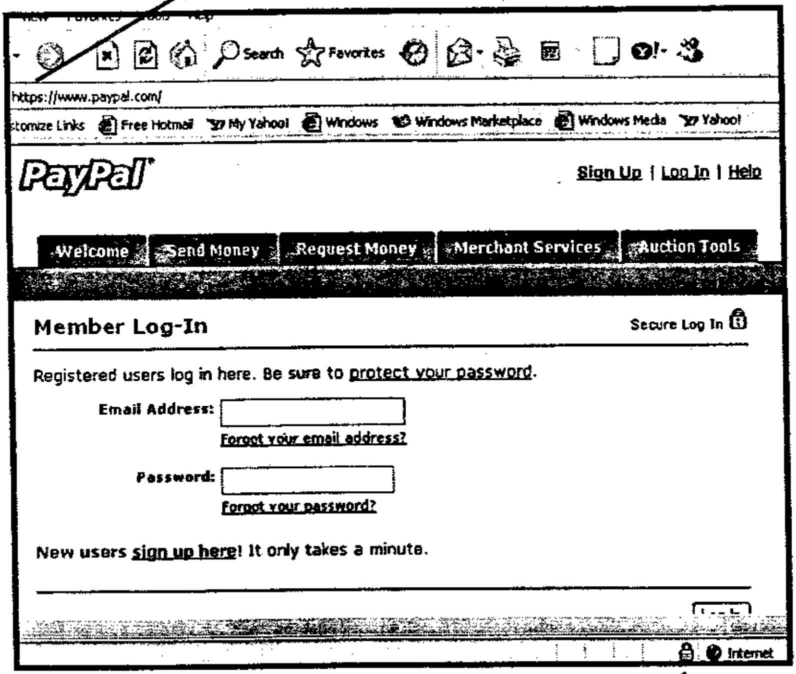
وكما ذكرنا سابقاً إن بروتوكول **S-HTTP** هو نسخة أمنية من بروتوكول **HTTP** ويُستخدم للاتصال مع مواقع الويب.

يعمل بروتوكول **S-HTTP** بين طبقة **TCP/IP** وبروتوكول **HTTP**. فعندما يطلب بروتوكول **HTTP** إرسال معلومات إلى مخدم آخر، يقوم بإرسال الطلب إلى بروتوكول **S-HTTP** ليتحقق من أن المعلومات مشفرة وصحيحة قبل إرسالها إلى بروتوكول **TCP/IP** ليقوم بنقلها.

فمثلاً : إذا أردت أن تدخل على موقع مثل **paypal** وتقوم بتسجيل إسم المستخدم وكلمة السر فلابد أن تتأكد أن **//:http** تحتوى على حرف **s** أى لابد أن يظهر الموقع بشريط العنوان بهذا الشكل

<u>httpS://www.paypal.com</u>

حرف S بجوار https://



هذا شكل القفل أيضاً بموقع **paypal**

ومن هنا أنت قد لاحظت أن **http://** بها حرف **s** لتكون **https://**

فكثير من الرسائل المغرضة للإختراق قد تأتى إليك مثلاً بأن تقوم بعملية تأكيد معلوماتك فى خلال ساعات وإلا سوف يعلق موقعك **suspended** ويعطيك لينك لكى تضغط عليه لتقوم بعملية

التسجيل فتقع فى الفخ وتقع فريسة للكراكرز عديمى الضمير والإخلاق ، لذلك إذا قمت بالضغط على هذا اللينك فتأكد أن الموقـــع الـــذى سيظهر لك به حرف S مثال **https://** وإن لم يظهر لك هذا الحرف فتأكد مائة فى المائة أنه فخ ..

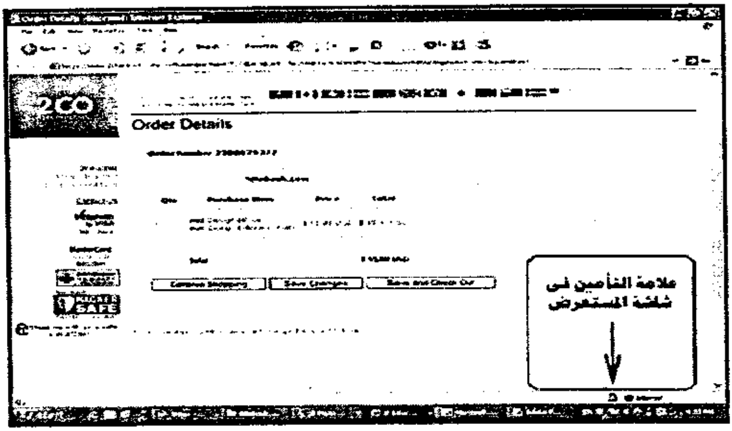
ولكن الأصوب أخى المستخدم أن لا تدخل أبداً إلى موقع بالإنترنت من خلال رسالة إيميل **E-mail** .

المثال الثانى : وجود شكل القفل بالشريط الأسفل

هو دليل على أن هذا الموقع محمى ببروتوكول **SSL**

للتأكد من تأمين عملية الشراء الإليكترونية باستخدام البطاقة الائتمانية عبر الانترنت فى أى موقع قم بإجراء الخطوات التالية:

- عند الضغط على زر الشراء سيتم فتح موقع شاشة الدفع باستخدام البطاقة الائتمانية مثال موقع **2checkout** أو موقع **stormpay** أو **e-gold** أو حتى موقع **paypal** إن كنت من قاطنى الدول المدرجة لها، ستظهر شاشة الشراء وإدخال البيانات كما بالشكل التالى.
- بالنظر إلى الشريط السفلى الموجود فى نافذة برنامج المستعرض (انترنت اكسبلورر) على سبيل المثال.



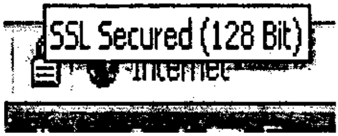
- سوف ترى قفل ذهبى صغير فى الشريط ، وهذا الشريط يدل على أن هذا الموقع مؤمن للشراء ويحتوى على بروتوكول سرية البيانات **SSL** كما بالشكل



قم بالوقوف بمؤشر الماوس فوق القفل مباشرة فيظهر لك مربع أصفر صغير فوق القفل يشير إلى بروتوكل التشفير المستخدم . (و من المعروف أن بروتوكل التشفير المستخدم فى تأمين البيانات على مواقع الويب هو :

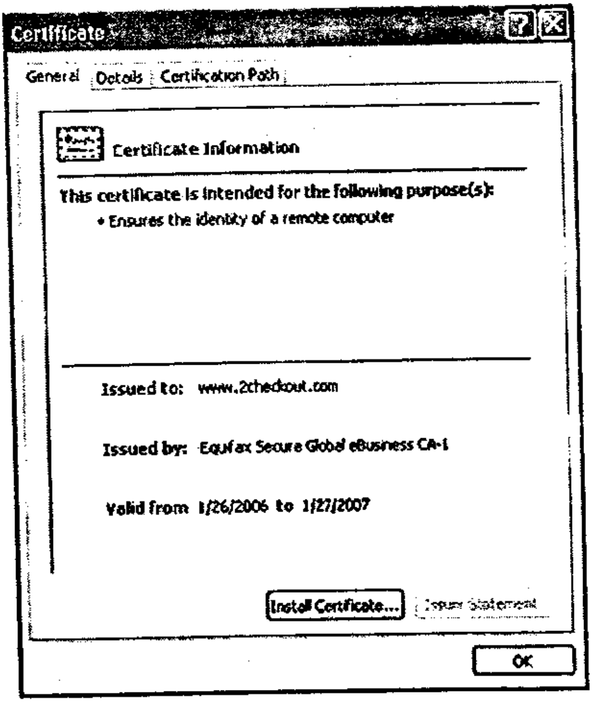
بروتوكول طبقة التأمين ***SSL*** أو ***Secure Socket Layer***) أما

الرقم ١٢٨ فهو عدد الــ**bits** المستخدمة فى التشفير وهو رقم عالى فى عملية التأمين.



بهذا تكون قد تأكدت من تأمين عملية البيع الاليكترونية فى أى موقع للبيع الاليكترونى.

ولزيادة التأكد من أن شهادة التأمين مصدرة فعلياً للجهة التى تمنحها بيانات بطاقتك الائتمانية، يمكنك الضغط بمؤشر الماوس مرتين متتاليتين على القفل الذهبى نفسه ليتم فتح نافذة مربع صغير به بيانات شهادة التأمين (يرجى قراءة السطر الخاص بإصدار الشهادة) ومطابقته بإسم مانح خدمة الشراء الاليكترونى مثال **2CheckOut** أو خدمة تقوم باستلام النقود أون لاين **Online** كما بالشكل :



ملحوظة :

بروتوكول SSL

يقوم بروتوكول SSL بإنشاء طبقة إرسال خاصة بدلاً من إستخدام

بروتوكولHTTP ، مما يعني أن بمقدور النظام العمل مع أي من بروتوكولات الإنترنت، بما في ذلك **HTTP** و **FTP** و **Telnet** و **Gopher** يعمل بروتوكول **SSL** من خلال تأسيس قناة اتصال آمنة ومنفصلة لكافة الرسائل التي تستخدم بروتوكول **HTTP** ويتم إعداد هذه القناة الآمنة على المخدم وعلى المتصفح بواسطة برمجيات **SSL**خاصة.

بروتوكول الحركات المالية الآمنة SET

طوَّرت مجموعة من الشركات العالمية الرائدة (منها مايكروسوفت، وآي بي إم (IBM)، وفيزا (VISA)، وماستر كارد (MasterCard) بروتوكولاً لعمليات الدفع (payment protocol)، أطلقت عليه اسم بروتوكول الحركات المالية الآمنة (Secure Electronic Transactions - SET). والغاية من هذا البروتوكول ضمان الحفاظ على أمن البيانات (خصوصيتها وسلامتها (integrity) والتحقّق من وصولها إلى الجهة المطلوبة) أثناء إجراء الحركات المالية (Financial transactions) عبر شبكة مفتوحة مثل الإنترنت. ويشبه هذا البروتوكول– إلى حد كبير– بروتوكولَ الطبقات الأمنية (Secure Socket Layers- SSL) في إستناده إلى التشفير والتواقيع الرقمية .

وللحفاظ على خصوصية وسلامة المعلومات المنقولة عبر الإنترنت بين الزبائن وهم حاملي بطاقات الإئتمان (cardholders) والتجّار (Merchants)، يستخدِم بروتوكول الحركات المالية الآمنة (SET) برمجيات تُدعى برمجيات المحفظة الإليكترونية (electronic wallet software). وتحوي المحفظة الإليكترونية رقم حامل البطاقة (cardholder number)

والشهادة الرقمية (**digital certificate**) التابعة له، أما التاجر، فتكون له شهادة رقمية صادرة عن أحد البنوك المعتَمَدة. ويستخدم كل من حامل البطاقة والتاجر الشهادة الرقمية التابعة له، مما يتيح لكل منهما التحقق من هوية الآخر عند إجراء الحركات المالية عبر الإنترنت.

وإلى جانب شركتي فيزا وماستركارد ، هناك حالياً العديد من الشركات العالمية التي تدعم هذا البروتوكول، ومنها :

مايكروسوفت **Microsoft** ،

نتسكيب **Netscape**

فيري ساين (***Verisign***)

(Systems Teresa).

عملية الشراء وفقاً لبروتوكول الحركات المالية الآمنة (SET)

تتضمّن عملية الشراء وفقاً لبروتوكول الحركات المالية الآمنة (**SET**) خمسة أطراف أساسية هي:

١. حامل البطاقة الإئتمانية (**cardholder**) – وهو الزبون
٢. موفّر المحفظة الإليكترونية (**electronic wallet provider**)
٣. التاجر (**Merchant**)
٤. معالج عمليات الدفع (**acquirer or payment processor**)
٥. بوابة الدفع (**payment gateway**).

وحامل البطاقة (**cardholder**) هو شخص لديه حساب بطاقة ائتمانية (لدى فيزا أو ماستر كارد). ويستخدم هذا الشخص محفظة إليكترونية تحوي شهادات رقمية لبروتوكول الحركات المالية الآمنة (**SET**). وحاملُ البطاقة هو الزبون (**customer**) في هذه العملية.

موفّر المحفظة الإليكترونية (electronic wallet

(provider فهو المؤسسة المالية التي تزوِّد الزبائن بالأدوات التي تُتيح- بشكل آمن- شراء البضائع والخدمات عبر الإنترنت. ومن هذه الأدوات الشهادات الرقمية، أو شهادات بروتوكول الحركات المالية الآمنة (**certificates SET**).

التُجار (**merchants**) فهم الشركات والأفراد الذين يعرضون هذه البضائع والخدمات عبر الإنترنت. وكي يتمكَّن هؤلاء التجار من التجاوُب مع الحركات المالية التي يقوم بها الزبائن، لا بُدَّ لهم من الإرتباط بعلاقة مع معالجي عمليات الدفع (**payment processors**) أو مؤسسات مالية معتَمَدة أخرى.

معالج عمليات الدفع (**acquirer or payment processor**) وهو المؤسسة المالية التي تزوِّد التُجار بالحسابات (**accounts**)، وتتولّى التحقّق من عمليات الدفع التي قام بها الزبائن، بالإضافة إلى التعامل معها ومعالجتها.

بوابة الدفع (**payment gateway**) هي الجهاز الذي يشغِّله معالج عمليات الدفع (**acquirer**).ويتولى هذا الجهاز معالجة رسائل الدفع التي يتلقّاها من التجار، وأوامر الدفع التي يتلقّاها من حاملي البطاقات.

إجراء الحركات المالية وفقاً لبروتوكول الحركات المالية الآمنة SET

يقوم الزبون في أول الأمر بفتح حساب بطاقة ائتمانية (credit card account) (ماستر كارد (MasterCard) أو فيزا (VISA)) في أحد البنوك، ثم يُصدِر البنك إلى صاحب البطاقة برنامجاً خاصاً ببروتوكول الحركات المالية الآمنة (SET) يُدعى برنامج المحفظة الإليكترونية. وتُستخدَم هذه المحفظة في الشراء وإجراء الحركات المالية عبر الإنترنت. وتُثبَّت المحفظة الإليكترونية في كمبيوتر المستخدِم، حيث يُمكن له الدخول إليها في أي وقت للقيام بعملية الدفع عبر الإنترنت. وتحوي هذه المحفظة معلومات مثل رقم البطاقة الائتمانية (credit card number)، وشهادة بروتوكول الحركات المالية الآمنة (SET certificate)، وتاريخ إنتهاء البطاقة، إضافة إلى معلومات أخرى. ويمكن تنزيل برنامج المحفظة من الإنترنت، ويكون هذا البرنامج مؤمَّناً بكلمة مرور pass word . ومن جهة أخرى، تُعَدّ شهادة بروتوكول الحركات المالية الآمنة (SET certificate) دليلاً على أن البنك قد تَحقّق من هوية حامل البطاقة. وللحصول على هذه الشهادة، يُحوَّل الزبون إلى جهة مخوَّلة بمنح الشهادات ومعتَمَدة لدى البنك. ويفتح التاجر حساباً لدى معالج عمليات الدفع (payment

processor) الذي يختاره (قد يكون بنكاً)؛ ليحصُل على ما يلزمه من برمجيات لإستخدام بروتوكول الحركات المالية الآمنة. وتتضمَّن هذه البرمجيات شـــهادة بروتوكـــول الحركـــات الماليـــة الآمنـــة (SET certificate) الممنوحة للتاجر، والمفتاح العام (public key) لمعالج عمليات الدفع المختار. وتُستَخدَم هذه البرمجيات لمعالجة الحركات المالية على الإنترنت.

وللحصول على اى معلومة تخص برامج الحماية وتحميلها وتحديثها مجاناً برجاء زيارة موقعنا على الإنترنت

www.books4internet.com

أو زيارة المنتدى مباشرة

www.books4internet.com/vb

كل ما عليك فعله أن تقوم بتسجيل بريدك الإليكترونى

وإسم المستخدم وكلمة السر للدخول

بعدها

يمكنك الدخول وقم بإرسال أية أسئلة خاصة

بالتجارة الإليكترونية و أمن المعلومات

أو أى موضوع خاص بالكمبيوتر والإنترنت

وتكنولوجيا المعلومات

المشرفين على المنتدى مهندسون متخصصون

الآن إذهب إلى موقعنا

www.books4internet.com

لترى أيضاً العروض والخصومات الخاصة بكتب المركز

وأيضاً يمكنك التسجيل لحضور ندوات مجانية عن التجارة الإليكترونية.

الفصل الثامن

طرق أمن المعلومات والحفاظ على البيانات

١ - طريقة لوضع كلمات سرية لملفات الوورد

تستطيع ذلك وبدون استخدام أي برنامج .. فمثلا لا يوجد من لا يستخدم برنامج وورد تبع الأوفيس .. أغلبنا نستخدمه هذا إذا لم يكن الجميع .. فبعملك على برنامج وورد سوف تحتاج بالتأكيد في بعض الأحيان إلى توفير بعض الخصوصية لمنع الآخرين من معرفة أسرارك الشخصية أو أسرار عملك .. فهذا هو الحل :

أولاً : عليك أن تفتح المستند الذي تريد أن تضع له كلمة سر والذي تريد أن تمنع الآخرين من الإطلاع عليه أو عملية تخريب..

ثانياً : من القائمة الرئيسية أضغط على ملف(File)
ثم اختر حفظ في.. .. (Save As)

ثالثاً : سوف تفتح لك نافذة الحفظ لا تحفظ الآن انتظر .. من خلال صفحة الحفظ ابحث عن كلمة أدوات(Tools)
وسوف تجدها في الأعلى .. أضرب على لسان التبويب بتاعها وعندها سوف ينسدل لك لسانه اختر الآن (General Option)

رابعاً : سوف تفتح لك نافذة .. أنظر إلى الأسفل سوف تجد مستطيلين الأول بعنوان **(Password to open)**

وهنا ضع كلمة السر التي تريدها .. والمستطيل الآخر بعنوان **(Password to modify)**

(OK)وهنا كرر كلمة السر السابقة .. ثم اضغط على زر موافق..

خامساً : بعد ضغطك زر**(OK)**

سوف يظهر لك مربع آخر بنفس عنوان المستطيل الأول السابق الذكر ما عليك سوى كتابة كلمتك السرية السابقة ،، ثم اضغط**(OK)**

..أيضا سوف يظهر لك مربع أخير بنفس عنوان المستطيل الثاني السابق الذكر ،، ما عليك سوى تكرير كلمتك السرية ،، ثم اضغط على **OK**

سادساً : الآن أختر المكان الذي تريد أن تحفظ مستندك فيه ،، ثم اضغط على زر ..حفظ **(Save)**

..وبهذا تكون قد حفظت الملف المحمي بكلمة سر..

ثانياً : طريقة لإخفاء الـ IP الخاص بجهازك

وذلك حتي تتجنب أخطار الهاكرز والمحترفين وتكون في أمان ولكن هذا الأمان من اختراق الجهاز وليس الفيروسات .

لذلك لابد من وضع برامج حماية ممتازة جدا بحيث يصعب اختراقها ولتنفيذها :

انقر **Click** شمال علي **Start** ثم اختر بالنقر **Click** شمال علي **Run** ثم اكتب **Cmd**

ثم اضغط علي **Enter** سوف تفتح واجهة الدوس

ثم اكتب **drwatson** في الواجهة المفتوحة ثم اضغط علي مفتاح **Enter** من لوحة المفاتيح سوف يتم إخفاء **IP** الخاص بالجهاز فورا ويظهر مربع حوار يخبر بذلك أتركة مفتوح

بالطبع رقم الـ **IP** لا يختفى بالنسبة لك أنت ولكن هذا الرقم يختفى لأى مخترق آخر ..

وللحفاظ على البيانات

البيانات المخزنة على الحاسبات هي أغلي ما يوجد داخل وحدات التخزين و هي أكثر أهمية من البرامج و التطبيقات مهما كانت قيمتها، لأن فقدها يعني عدم إمكانية إستعادة هذه الملفات مرة أخري، و قد تزداد المشكلة أكثر إذا لم يكن في استطاعتنا إدخال البيانات للحاسب مرة ثانية من النسخة الورقية.

و على الرغم من أن التقنية الحديثة المستخدمة في صناعة وحدات التخزين الرئيسية **Hard Disk** تطورت تطوراً كبيراً بحيث

أصبحت تلك الوحدات تعيش لفترات أطول كما صارت سعتها التخزينية أكبر و زادت سرعتها بدرجة كبيرة إلا أن معدلات حوادث فقد البيانات لا تزال في إزدياد . و تعتبر أعطال وحدات التخزين الرئيسية التي تعتمد على تقنية السطح المغناطيسي في حفظ البيانات مسئولة عن نسبة كبيرة من هذه الحوادث و ذلك بالإضافة إلى الأخطاء البشرية من المستخدمين .

اساليب الوقاية

و حتى لا تقع ضحية لفقد ملفاتك من على الحاسب الخاص بك يجب أن تراعي النقاط التالية :

١- وحدة التخزين الحديثة و التي أصبحت ذات سعة أكبر من وأحدث حيث صارت تخزن أعداداً هائلة من الملفات . فيقدر الخبراء أن سعة وحدات التخزين أصبحت أكبر ٥٠٠ ضعف عما كانت عليه منذ عشر سنوات . و كلما زاد عدد الملفات التي يتم الإحتفاظ بها على وحدة التخزين الواحدة كان ذلك يعني أن مشكلة تلف هذه الوحدة ستصبح أخطر لأنها تحتوي على آلاف الملفات .

و إذا حدث إنقطاع مفاجئ للتيار الكهربائي أثناء تحرك رأس القراءة و الكتابة على السطح المغناطيسي للوحدة فإن ذلك قد يسبب إحتكاكاً شديداً بين رأس القراءة و الكتابة و السطح الحساس للوحدة مما قد

يتسبب في تلفها.

٢- الإختراعات الحديثة جعلت الإنسان يقوم بتخزين معلومات و بيانات أكثر على الحاسبات الإليكترونية فوسائل إدخال البيانات للحاسب تنوعت فبجانب لوحة المفاتيح التي يمكنها إدخال الحروف و الأرقام يمكننا أن نستخدم الماسح الضوئي لإدخال الصور و المستندات و نستخدم الكاميرات الرقمية **digital camera** و كاميرات الفيديو لإدخال الصور و الأفلام . كما أصبحت شبكة الإنترنت مصدراً جديداً للمعلومات التي يمكن تخزينها على ا لحاسب .

و بصفة عامة فإن الإعتماد الكبير على تخزين مختلف أنواع البيانات على الحاسبات الإليكترونية وضع بعداً جديداً لحوادث فقد البيانات نتيجة لعيوب تصنيع و استخدام وحدات التخزين أو للأخطاء البشرية حيث صار حجم المعلومات التي يمكن أن نفقدها كبيراً بشكل مؤثر نظراً لاعتمادنا على الحاسبات في تخزين كل المعلومات التي نتعامل معها و لذا فإن فقد هذه البيانات أو عدم التمكن من الوصول إليها يعني أن قطاعات مهمة من المجتمع يمكن أن تتوقف عن العمل نتيجة لحوادث فقد البيانات.

٣- إستخراج نسخة إحتياطية **Backup** من الملفات هي الطريقة الوحيدة التي يمكننا أن نعالج بها مشاكل فقد البيانات، و لكن للأسف أن التقنية الحديثة المستخدمة في الحصول على النسخ الإحتياطية لم

تستطع أن تقدم الحل الشافي لهذه النوعية من المشاكل و ذلك رغم الجهود الكبيرة التي بذلت في هذا ا لمجال فكثير من المستخدمين يكتشفون عند تعرضهم لفقد البيانات أن النسخ الإحتياطية التي يحتفظون بها قد أصبحت عديمة الفائدة نظراً لأنها غير كاملة أو غير حديثة أو تم استخراجها بطريقة خطأ و لم نعرف بهذا العيب إلا عندما وقعت المشكلة و حاولنا إعادة الملفات المفقودة.

الفصل التاسع

الثغرات

هناك ثغرات وطرق كثيرة تمنع حتى المواقع الـتى تكشـف الثغـرات المفتوحة في جهاز الضحية من كشفها لأنه حتى تلك المواقع تعتمد على قاعدة بيانات تحتوي على معلومات محدده لديها .

فهنا ما زالت المشكلة تتفاخم ، حيث ضعفاء النفوس الـذين يـدعون أنفسهم بالهاكرز إستدلوا ويستدلون على طرق عديدة تعتمـد علـى ثغرات أنظمة التشغيل من خلالها يصلون إلى المعلومات السرية مثـال المعلومات الخاصة بتداول الأسهم والحسابات الشخصية وحسـابات البنوك وأرقام بطاقات الإئتمان وغيرها.

وأحد أخطر الطرق المنتشره عند الهاكرز هو إستخدام أحـد ثغـرات أنظمة تشغيل الكمبيوتر في إرسال برامج التجسس وغيرها من بـرامج أدوات الهاكرز ، طبعاً بعد تغيير بصمة برنامج التجسس المرسل لكي لا يكتشفه برنامج الحماية.

و من المعروف أنه إذا تركت جهاز الكمبيوتر متصل علـى الإنترنـت لبضع ساعات سوف تجد ملف تجسس لأنه في أى لحظة قـد يسـتقبل ملفات تجسس ، هذه الثغره في نظام التشغيل تتيح للـهاكرز إرسـال برامج التجسس بطريقة عشوائية لأي كمبيوتر متصل بالإنترنت.

اولاً : ثغرات موجودة فى ويندوز إكس بى window xp

هناك ثغرات في أجهزة الإكس بي و دائماً تكون مدخل للهاكرز والكراكرز ومعظمنا لايعرفها ولا كيف يمكن التخلص من هذه الثغرات الموجودة في **xp**

الثغرة الاولى :

تعتبر إحدى البوابات الخطيرة للفيروسات وملفات التجسس

وللتخلص من هذه الثغرة :

١- إذهب إلى لوحة التحكم **panel control**

٢- ثم خيارات المجلد **folder options**

٣- ثم أنواع الملفات **file types**

وهناك ستجد :

Windows script host setting file

قم بحذفه فوراً

الثغرة الثانية :

وتسمى (مشاركة ملفات بسيطة) **simple file sharing**

ولكن تفعيلها ليس بسيطاً بل هو خطير جداً ..

إتبع الآتى :

١- من خيارات المجلد **folder options**

٢ - ثم عرض **view**

٣ - يجب إزالة علامة الصح من داخل المربع أمام :

مشاركة ملفات بسيطة (ينصح بذلك) .

(use simple file sharing) (recommended)

الثغرة الثالثة :

وتسمى : (عدم حفظ الصفحات المشفرة إلى القرص).

save encrypted page to disk

إتبع الآتى :

١- لوحة التحكم **control panel**

٢- خيارات انترنت **options internet**

٣- خيارات متقدمة **advanced**

٤- وضع علامة صح داخل المربع :

(عدم حفظ الصفحات المشفرة إلى القرص)

don't save encrypted page to disk

ثم موافق.

ثانياً : ثغرة امنية حرجة في متصفح الإنترنت لمايكروسوفت

Microsoft Internet Explorer

تم إكتشاف خطأ برمجي في متصفح الإنترنت لمايكروسوفت تمكن بعض المواقع من تثبيت مكونات جديدة للنظام إما ان تكون **ActiveX** او **dll** تستخدم لتنفيذ أمر برمجي.

ثالثاً : ثغرة امنية خطيرة Heap Overflow في متصفح الانترنت لمايكروسوفت

الثغرة الأمنية في مكونات ويندوز **COM Object** تسمح بإنشاء صفحه إنترنت يستطيع من خلالها إنزال وتشغيل ملف تنفيذي في جهاز المستخدم

الأنظمة المصابة

Windows 2000 Server SP4 , Internet Explorer 6.0 SP1
Internet Explorer 6.0 SP1 ، Windows XP SP2

خطورة هذه الثغرة أنه لايوجد أي تحديث أمني إلى الآن.

ماذا بعد

هل شركات أنظمة التشغيل لا تدرى أن هناك ثغرات فى أنظمتها بالطبع هى تعلم ذلك بل و تصرح بين الحين والآخر بأنها قضت على ثغرات نظامها..

ولأننا جميعاً مؤمنين بأن هناك ثغرات كثيرة تسمح لضعفاء النفوس بالتطفل على خصوصياتنا ، ونعرف تماماً مدى سهولة حصول الهاكرز

على هذه البرامج . فهناك برامج هاكرز مختصة باستخدام ثغرات مايكروسوفت والبال توك والماسنجر والبرامج التى تحتاج للتحديث وغيرها .

فبمجرد إستخدام برنامج مثل **Super Scan** أو غيره من البرامج وهي كثيرة وسهلة الحصول عليها مجاناً من خلال مواقع الإنترنت أو الآت البحث ، وذلك للبحث عن المنافذ المفتوحه (**Port**) في جهاز الكمبيوتر الخاص بنا. وبعدما يجد الهاكرز المنفذ المفتوح يستخدم البرنامج الخاص بذلك المنفذ ، وهناك طرق تستخدم من قبل كبار الهاكرز للإختراق دون الحاجة لبرامج الإختراق ودون الحاجة لمعرفة المنفذ (**Port**) فإما عن طريق معرفة رقم الـ **IP** أو بطرق الإرسال العشوائي ، وبالنسبة للهاكرز إن برامج الحماية من خطر الإنترنت تعتمد على بصمة الملفات فقط وأي هاكر يستطيع تغيير بصمة برنامجه بحيث لا تتعرف برامج الحماية على تلك الملفات وذلك من خلال برامج الهاكرز المختصة بتغيير بصمة البرامج.
والدليل إن الكثير من الأجهزة و الشبكات العالمية والبنوك تم إختراقها ولو كانت هذه البرامج ذات فعالية لتمكنت من حماية البنوك والشبكات والجامعات المختلفة وشركة الإتصالات .

إذاً ما هو الحل

نعتبر أن هؤلاء الهاكرز والكراكرز الذين يضرون أجهزتنا ويخترقون مواقعنا ويسرقون نقودنا هم بالفعل أناس لا ضمير ولا أخلاق لهم ، لذلك لابد من أخذ الحيطة لحماية سرية المعلومات الخاصة بأجهزتنا ومواقعنا وشبكاتنا و ببرامج التداول المالية عبر الإنترنت بما فيها الأسهم والبورصات والتعاملات المالية كالحسابات البنكية وبطاقات الائتمان وغيرها .

لذلك يجب إستخدام برامج لحماية الأجهزة وحماية المواقع وحماية الشبكات كبرامج درع الفيروسات **System Virus Armor** للتخلص منها أو عدم دخولها وذلك طبقاً للتقنيته العلمية المستخدمه للحماية .

والفصل القادم يقدم لنا أهم برامج الحماية التى يجب الإستعانه بها (بعضها طبعاً وليس كلها) .

الفصل العاشر

برامج الحماية

اولاً : برامج حماية الاجهزة :

يمكنك تحديث هذه البرامج وتركيبها بجهازك مجاناً

- برنامج الحماية **BitDefender 8**
- تحديث لـبرنامج **PC-Cillin**
- برنامج الحماية **McAfee 8**
- برنامج الحماية **Panda**
- برنامج **Ad-Aware SE**
- برنامج **eTrust EZ Anti-Virus**
- برنامج **The Cleaner**
- برنامج **Kaspersky Anti-Virus**
- تحديث برنامج لـ **Norton AntiVirus**
- برنامج **Trojan Remover**
- برنامج **F-Prot Antivirus**
- برنامج **AVG Anti-Virus 7**

وايضاً يوجد كم هائل من برامج الجدران النارية

Firewall التى تؤمن وتحمى جهازك من التلصص والتجسس والسرقة (الكراكرز) ومن المتطفلين(الهاكرز) مثال :

- برنامج **R-Firewall 1**
- برنامج **Outpost Firewall pro 4**
- برنامج **Ashampoo Firewall 1**
- برنامج **BlackICE PC protection 3.6**
- برنامج **Comodo personal Firewall 2.3.5.62**
- برنامج **Core Force**
- برنامج **Hackaer Smacker 2**
- برنامج **Look'n stop 2.05**
- وأخيراً برنامج

McAfee Personal Firewall plus v.5.0.1.5

ثانياً : برامج لإدارة كلمات السر

هناك أيضاً برامج كثيرة يمكنك تحميلها أو تحديثها من مواقع الإنترنت المختلفة ، مثال هذه البرامج :

١. برنامج **PassWord manager**

برنامج يدير كلمات السر فى جهازك وتخزينها

٢. برنامج **1st screen lock**

يمكنك هذا البرنامج لعمل كلمات سر لحماية جهازك وشبكة الإنترنت.

٣. برنامج **Hidesfiles 1.1**

بهذا البرنامج يمكنك أن تخبيء ملفاتك بطريقة آمنة ، وبهذه الطريقة لا يمكن لأحد أن يسرق معلوماتك .

٤. برنامج **Excel pass word recovery 1**

برنامج لكسر تشفير ملفات الإكسيل

٥. برنامج **OutLook password v.9**

إستعادة كلمة السر فى برنامج **out look** عند فقدانها

٦. برنامج **IE internet security**

برنامج لحماية كلمات السر المستخدمة فى المتصفح **browser**

٧. برنامج **KeyPass 4.2.2**

برنامج يدون لك كلمات المرور الخاص بك ويحفظها ويديرها مهما كانت كثرتها .

٨. برنامج **Face Code v2.1.4**

من أهم برامج حماية جهازك ومعلوماته حيث أنه بهذا البرنامج

يمكنك تخزين صورتك به ليكون وجهك هى كلمة السر للدخول لجهازك وذلك طبعاً يستلزم وجود كاميرا.

٩. برنامج **safe input 1.2**

إن كنت ممن تقوم بعملية الشراء والبيع عبر شبكة الإنترنت فهذا البرنامج هام جداً لك ، حيث أنه يكشف ملفات التجسس التى تدخل إلى جهازك أثناء كتابتك لكلمات السر.

١٠. وأخيراً برنامج **Windows Guard**

الذى يمكنكم من حماية كلمة السر الخاصة ببرامجك وويندوز.

ثالثاً : برامج لمكافحة التجسس

١. برنامج **A2freesetup**

هذا البرنامج له قدرة على الإستكشاف وله القدرة على إزالة التروجان **Trojan**

٢. برنامج **Advanced spyware remover**

لمكافحة ملفات التجسس

٣. برنامج **Anti Trojan Elite**

أسرع برنامج فى البحث عن ملفات التجسس وأحصنة طروادة **Trojan** والديدان **worms** وهذا البرنامج يجمع بين

الحماية والتسريع والتصليح ..

٤. برنامج **Defense wall 1.65**

وهو برنامج دفاعى يقاوم ملفات التجسس **spy ware** والتروجان **Trojan**

٥. برنامج **Anti worm**

لكشف وحذف ملفات التجسس مثل **worms** و **Trojan**

رابعاً : برامج تشفير الملفات

١. برنامج **Dekart private desk**

يجعل الملفات غير مرئية باستخدام عملية تشفيرمحمية

٢. برنامج **File Buddy**

يسمح هذا البرنامج بتشفير الملفات ثم فكها بسهولة

٣. برنامج **easy file and folder protector**

يقوم بتشفير الملفات وإخفائها بشكل آمن .

٤. برنامج **Folder lock**

أيضاً يقوم بإخفاء الملفات برقم سرى وحمايتها من المتطفلين.

٥. برنامج **Masker 7**

يقوم أيضاً بعملية تشفير الملفات وإخفائها بكلمة سر

كيفية الحصول على برامج الحماية مجاناً :

يمكنك الذهاب إلى مواقع التحديث المجانى أو مواقع المنتديات التى تقدم هذه التحديثات المجانية وليتم عمل هذا إتبع الخطوات الآتية :

١. قم بالدخول إلى آلات بحث تدعم اللغة العربية مثال

- جوجل www.google.com.eg
- أو موقع أرابو www.arabo.com
- أو موقع أرابى www.araby.com

٢. أكتب فى خانة البحث باللغة العربية : " برامج الحماية "

٣. سيظهر لك مئات المواقع والمنتديات المصاحبة لها تقدم خدمة تحديث برامج الحماية مجاناً ومثال لهذه المواقع :

- www.books4internet.com
- www.absba.com
- www.arabsgate.com
- www.sultan.org
- ومواقع كثيرة أخرى قم بإكتشافها بنفسك

٤. حينما تجد نفسك داخل إحدى هذه المواقع ستبدأ البحث

وغالباً ما ستجد الموضوع الذى تبحث عنه فى أول نافذة كما هو الحال إذا كان الموضوع الذى تبحث عنه داخل مواضيع المنتدى الخاص بالموقع ..

٥. معظم أصحاب المنتديات يطلبون منك أن تسجل بالمنتدى قبل الدخول لرؤية الموضوع ، قم بالتسجيل بلا خوف . فقد أصبحت المنتديات هذه الآونه من أهم الأماكن داخل شبكة الإنترنت التى منها يمكنك أخذ كم هائل من المعلومات والبرامج مجاناً.

الفصل الحادى عشر

الحماية المتكاملة لجهازك :

اولاً : تحتاج لهذه البرامج أن تكون بجهازك :

Norton AntiVirus 2002 -1

برنامج حمايه غني عن التعريف

2- برنامج The Cleaner

برنامج حماية من جميع السيرفرات المسربة للمعلومات – ويفضل ترقيتة كل فترة لتحديثه للقضاء على التروجانات والفيروسات

WinPatrol 3.2 -3

لمسح ملفات الكوكيز التي تضعها بعض المواقع في الاكسبلورر

4- برنامج Ad-aware v5.6

لمسح ملفات الكوكيز الموجوده ضمن الملفات والبرامج في جهازك

5- برنامج ZoneAlarm Pro

للحماية من الهاكرز

من إحتوى جهازه على هذه البرامج أعتقد أنه سيتمتع بحماية جيده ولكن

يجب القيام بتحديث البرنامج (١ و ٢ و٥) بشكل دائم.

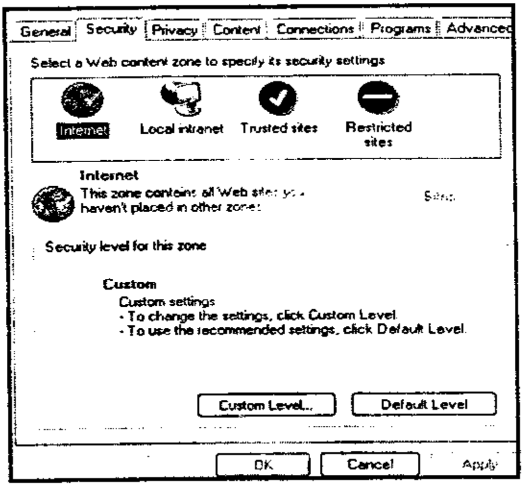
وطبعاً يمكنك إختيار برامج أخرى مشابهه لهذه البرامج ..

ثانياً : عدم تحميل المواقع الإباحية من خلال جهازك :

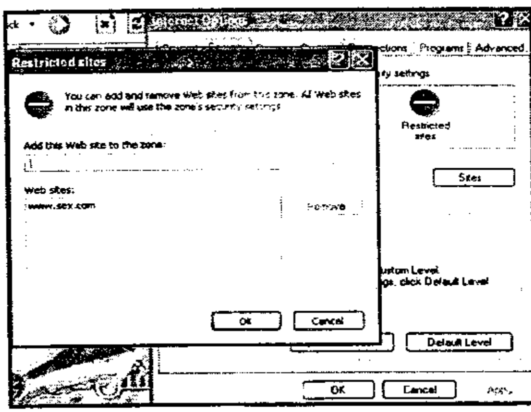
فى الحقيقة أن معظم الفيروسات وملفات التجسس يتم غرسها فى جهازك من خلال فتح أو تحميل المواقع الإباحية عن طريق جهازك ، لذلك يجب وضع برامج أو طرق لمنع تنزيل هذه المواقع إلى جهازك ، وهناك طرق كثيرة لمنع هذه المواقع نهائياً أن تدخل جهازك :

الطريقة الأولى : باستخدام اوامر ويندوز

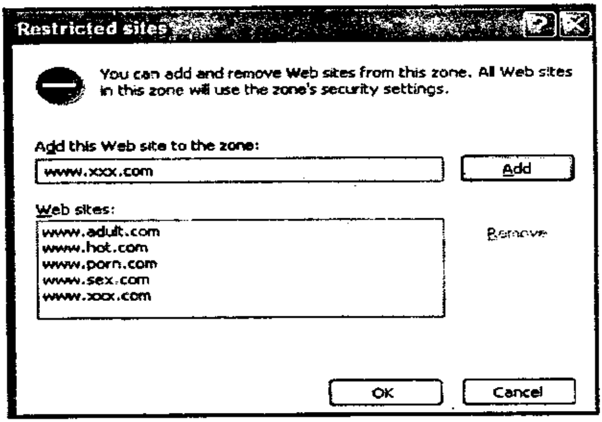
- إذهب إلى **Tools** من خلال المتصفح إنترنت إكسبلورر
- إختر **internet options**
- ستحصل على نافذة
- إضغط على **security** كما يلى:



- قم بالضغط على **Restricted sites**
- قم بالضغط على كلمة **sites** لتحصل على نافذة كما يلى:



• في خانة **add this sites to the zone** ضع كل المواقع الإباحية التي يشتبه بها ثم إضغط **OK** كما يلي :



الطريقة الثانية : باستخدام الآت البحث والدلائل

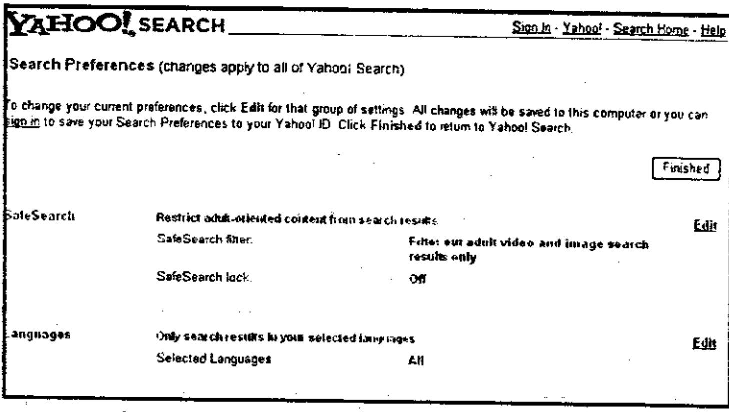
أحياناً ونحن نبحث داخل الشبكة تأتى إلينا إعلانات مخلة أو صور خليعة لكى نتلاشى كل هذا بل ولكى نمنع تماماً المواقع الإباحية من آلات البحث والدلائل ، يمكننا تغيير بعض خصائص آلة البحث لكى تمنع نهائى أى موقع إباحى حتى ولو حاولت بنفسك كتابة أى كلمة إباحية فلن يظهر أبداً هذا الموقع وهذا طبعاً يقينا ويقى أبنائنا من تلصص الأعداء الذين يريدون كسر عزائم أمتنا العربية وتسمى هذه العملية بعملية الفلترة **Filtration** ومعظم الآت البحث و الدلائل تملك

ضمن خصائصها هذه العملية التى ترشح أى موقع إباحى وعدم دخوله داخل متصفحاتنا .

و قد وفقنى الله سبحانه وتعالى فى جمع بعض هذه الآلات وكيفية تغيير وظائفها وخصائصها لنكون آمنين ونحن نعمل داخل الشبكة ومنها .

1- Yahoo: Set the Safe Search Filter option via page.Search Preferencesthe

بالدخول إلى موقع ياهو – قم بتسجيل الدخول – قم بالذهاب إلى **preferences** وفى خانة **safesearch** قم بالضغط على كلمة **edit** وحول كلمة **off** إلى كلمة **on**



إذهب إلى **search** ثم قم بالبحث عن أى كلمة إباحية أو حتى موقع إباحى لم تجد له أثر ، الآن أنت وأبنائك فى آمان .

2- Google: **See the SafeSearch help page for instructions on setting up filtering on a permanent or as-needed basis.**

بنفس طريقة ياهو قم بتغير الخصائص

3- AOL Search: **Doesn't appear to offer a filter, but enabling Parental Controls might have an impact on web search matches.**

4- Ask Jeeves: **Use options for Content Filtering on the Your Settings page or try Ask Jeeves For Kids, listed above.**

5- AltaVista: **Use the Family Filter Setup page.**

بنفس الطريقة إذهب إلى هذه الخاصية وقم بتغييرها

6- HotBot: **Use the Block Offensive Content section of the Filter Preferences page. Note that you may need to set this again if you change from using the default "HotBot" search engine that's offered.**

7- LookSmart: **LookSmart has never accepted**

adult content for listing within its directory results. However, obscure queries might bring these up in the crawler-based results that are sometimes provided.

8- Lycos: Use the Adult Filter section of the Advanced Search Filters page.

9- MSN Search: Use the Safe Search Filter on the Settings page.

10 - AllTheWeb: Use the Basic Settings page to enable the Offensive Content Filter option. The only works for searches in English.

الطريقة الثالثة : برامج منع المواقع الإباحية

Filtering and Blocking Software

أما هذه الطريقة فهى برامج تعمل من داخل الويب نفسه وليس فقط نتائج البحث .

وهناك برامج كثيرة تقوم بهذه المهمة ومن ضمن هذه البرامج ما يلى :

1- Cyber Patrol

http://www.cyberpatrol.com/

The program can filter web pages, newsgroups, chat rooms and other internet resources, and can be used to limit online time, create user logs and so on.

2- Net Nanny

http://www.netnanny.com/

Looksmart acquired Net Nanny in April 2004 and added porn-free web search to the product shortly thereafter. The product provides a wide variety of parental controls, including blocking content based on content, URL, or ratings. In addition to blocking web pages, the program allows selective blocking of access to chat, instant messaging, internet games and newsgroups. The program can also be configured to prevent illegal downloading of copyrighted or obscene material.

3- Web Blocker

www.web-blocker.com

برنامج جميل جداً لعدم فتح المواقع الإباحية
وإليك الشرح بالتفصيل :

قم بتنزيل وتثبيت برنامج
weblocker
http://www.web-blocker.com
من هذا الرابط . هذا البرنامج يقوم بمنع الدخول على المواقع الإباحية نهائيا . وهو برنامج رائع حقاً وخفيف ولا يقوم بالتأثير نهائيا على سرعة الإتصال . ويحتاج هذا البرنامج بعد تنزيله أن تكتب له كلمة سر . وسؤال سرى .

Password and secret question

لأنه من غير أحدهما لا يستطيع أحد أن يزيل البرنامج من على الجهاز المثبت عليه. وإذا حدث وحاول أحد أن يمسح ملفات البرنامج فإن البرنامج يمنع الدخول على الشبكة نهائيا ، إلى أن يقوم بإعادة تثبيت البرنامج من جديد .لكن يتبادر سؤال ، طالما أنا الذى سأضع كلمة السر هذه فربما راودني الشيطان ونفسى الأمارة بالسوء إلى إزالة البرنامج فى أى وقت ومعاودة المعصية مرة أخرى ؟ نقول بأنك لابد أن

تضع كلمة سر بحيث تنساها أنت نفسك ، وهذا بطريقة سهلة جداً

١ إفتح ملف وورد أو أى برنامج كتابة

٢ أغمض عينيك وأضغط على لوحة المفاتيح عشوائياً لمدة دقيقة مثلاً .

سينتج عن ذلك سطر طويل من الحروف الإنجليزية العشوائية .

٣ أختر بالفأرة من وسط هذا السطر أى جزء عشاوئيا " تقريبا ١٥ حرف مثلاً أو أقل أو أكثر قليلا

٤ قم بنسخ هذا الجزء ، ثم هناك فى البرنامج فى الجزء المخصص لإدخال كلمة السر (يطلب البرنامج إدخالها فى مكانين) ألصق ما نسخته

أنقر بالزر الأيمن للفأرة على المكان المخصص وأختر

paste أو أضغط **ctrl+v**

وفى مكان إدخال السؤال السرى أكتب أى شيء ، وفى مكان إجابة السؤال السرى يمكن أن تنسخ وتلصق جزء آخر من السطر الذى كتبته .

٥ أمسح السطر العشوائى الذى كتبته .

وبهذا تكون المهمة قد تمت بنجاح الحمد لله وأغلقت عن نفسك باب واسع للشيطان.

References

English refernces

- Ross J. Anderson: *Security Engineering: A Guide to Building Dependable Distributed Systems*, ISBN 0-471-38922-6
- Bruce Schneier: *Secrets & Lies: Digital Security in a Networked World*, ISBN 0-471-25311-1
- Robert C. Seacord: *Secure Coding in C and C++*. Addison Wesley, September, 2005. ISBN 0-321-33572-4
- Paul A. Karger, Roger R. Schell: *Thirty Years Later: Lessons from the Multics Security Evaluation*, IBM white paper.
- Clifford Stoll: *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, ISBN 0-7434-1146-3
- Stephen Haag, Maeve Cummings, Donald McCubbrey, Alain Pinsonneault, Richard Donovan: *Management Information Systems for the information age*, ISBN 0-07-091120-7
- Peter G. Neumann: *Principled Assuredly Trustworthy Composable Architectures* 2004
- E. Stewart Lee: *Essays about Computer Security* Cambridge, 1999

Internet websites

Search engines

Arabic books

Magazines

إصدارات المركز العلمي لتبسيط العلوم

م	إسم الكتاب	جنيه
١	موسوعة التجارة الإليكترونية (١)البيع والشراء عبر مواقع المزادات	١٥ج
٢	موسوعة التجارة الإليكترونية (٢) كيف تصمم موقع ناجح	١٢ج
٣	موسوعة التجارة الإليكترونية (٣) التصدير والإستيراد	١٢ج
٤	موسوعة التجارة الإليكترونية (٤) التسويق باستخدام البريد الإليكتروني	١٢ج
٥	موسوعة التجارة الإليكترونية (٥) كيف تبيع المنتجات العربية والإسلامية	١٠ج
٦	موسوعة التجارة الإليكترونية (٦) عملية الـ **Drop shipping**	١٠ج
٧	موسوعة التجارة الإليكترونية (٧) التسويق باستخدام الآت البحث	٨ج
٨	موسوعة التجارة الإليكترونية (٨) البرامج المشاركة	٩ج
٩	موسوعة التجارة الإليكترونية (٩)طرق الدفع عبر الإنترنت	١٠ج
١٠	موسوعة التجارة الإليكترونية (١٠) تعلم اللغة الإنجليزية التجارية	١٢ج
١١	موسوعة التجارة الإليكترونية (١١) خدمة العملاء عبر الإنترنت	١٠ج
١٢	موسوعة التجارة الإليكترونية (١٢) أمن المعلومات	١٠ج
١٣	موسوعة التجارة الإليكترونية مشروع (١) كيف تبيع **e-book**	٥ج
١٤	موسوعة التجارة الإليكترونية مشروع (٢) التعليم عن بعد	٥ج
١٥	موسوعة التجارة الإليكترونية مشروع (٣) عمل أرباح بواسطة **Google**	٥ج
١٦	موسوعة التجارة الإليكترونية مشروع (٤) **Pay per click PPC**	٥ج
١٧	موسوعة التجارة الإليكترونية مشروع (٥) **Pay per register**	٥ج
١٨	موسوعة التجارة الإليكترونية مشروع (٦) بيع الكتب عبر الإنترنت	٥ج
١٩	موسوعة التجارة الإليكترونية مشروع (٧) بيع منتجات الغير عبر موقعك	٥ج
٢٠	موسوعة التجارة الإليكترونية مشروع (٨) إستيراد المنتجات بأقل الأسعار	٥ج

٢١	موسوعة التجارة الإليكترونية مشروع (٩) تصدير المنتجات العربية	٥ج
٢٢	موسوعة التجارة الإليكترونية مشروع (١٠) كيف تسوق موقعك	٥ج
٢٣	Jobs online وكتابة السيرة الذاتية	١٠ج
٢٤	البحث داخل شبكة الإنترنت	١٠ج
٢٥	دليل المواقع التجارية	١٠ج
٢٦	دليل المواقع الصحية	١٠ج
٢٧	دليل المواقع العلمية	١٤ج
٢٨	2006 online sellers	١٠ج
٢٩	كيف تصبح مبدعاً (جديد ١٠٠%)	٩ج
٣٠	كيف تصبح مسوقاً ناجحاً (جديد ١٠٠%)	٩ج
٣١	كيف تصبح خبيراً فى صيانة الموبايل (جديد ١٠٠%)	٩ج
٣٢	كيف تصبح خبيراً فى الأسهم والبورصة (جديد ١٠٠%)	٩ج
٣٣	سلسلة مقارنات (١) عمرو و عمرو	٥ج
٣٤	سلسلة مقارنات (٢) أكاديمى و أكاديمى (وأعداد كثيرة أخرى)	٥ج
٣٥	Html والويب	٥ج
٣٦	Front page والويب	٥ج
٣٧	مايكروسوفت أوفيس والويب	٥ج
٣٨	فوتوشوب والويب	٥ج
٣٩	موسوعة أسرار الكمبيوتر والإنترنت رقم ١ مقدمة فى الحاسب الآلى	٧ج
٤٠	موسوعة أسرار الكمبيوتر والإنترنت رقم ٢ ويندوز windows	١٢ج
٤١	موسوعة أسرار الكمبيوتر والإنترنت رقم ٣ معالجة الكلمات وورد Word	١٠ج
٤٢	موسوعة أسرار الكمبيوتر والإنترنت رقم ٤ إكسيل Excel	١٠ج
٤٣	موسوعة أسرار الكمبيوتر والإنترنت رقم ٥ باور بوينت power point	١٠ج
٤٤	موسوعة أسرار الكمبيوتر والإنترنت رقم ٦ أكسيس Access	١٠ج

٤٥	موسوعة أسرار الكمبيوتر والإنترنت رقم (٧) إنترنت إكسبلورر	٧ج
٤٦	الإنترنت و أولادك	٧ ج
٤٧	ثورة الإنترنت	٧ ج
٤٨	دليل المواقع على الإنترنت	٧ج
٤٩	تعلم اللغة الإنجليزية من البداية إلى الإحتراف	١٢ج
٥٠	كن مسلماً عبر شبكة الإنترنت	٥ ج
٥١	كن داعياً عبر شبكة الإنترنت	٥ج
٥٢	كيف تستخدم الإنترنت لتقول للعالم من هو محمد (صلى الله عليه وسلم)	٥ج
٥٣	وافلسطين	٣ج
٥٤	العلم الحديث وأثره فى الدعوة الإسلامية	٥ج
٥٥	موسوعة أمراض العظام والكسور والعمود الفقرى	ج
٥٦	صيدلية فى كل منزل	٥ج
٥٧	شنطة سفر	٥ج
٥٨	رحلة إلى الصين	٥ج
٥٩	كومبو والشاطر نت	٥ج
٦٠	موسوعة كيف تشترى ؟	٥ج

دورات التجارة الإليكترونية - البيع والشراء عبر شبكة الإنترنت

١- دورة التأهيل للعمل بالتجارة الإليكترونية

- وورد **Word XP**
- طريقة البحث داخل الشبكة و عمل بريد إليكترونى وماسنجر
- اللغة الإنجليزية التجارية للعمل بها عبر الإنترنت

i. كيفية كتابة رسالة بريد إليكترونى **e-mail** باللغة الإنجليزية

ii. كيفية كتابة محتوى موقع **website** باللغة الإنجليزية

iii. مصطلحات التجارة الإليكترونية والإستيراد والتصدير

iv. مشروع التخرج

٢- دورات التجارة الإليكترونية

١- المستوى الأول

- ما هى التجارة الإليكترونية وما هى أنواعها وفوائدها
- البيع عبر مواقع المزادات والمخازن الإليكترونية
- وسائل الدفع المختلفة واهمها الدفع أون لاين **payment online**

٢- المستوى الثانى

- تصميم موقع ببرنامج فرونت بيدج ثم نشره داخل الشبكة
- عمل برامج مشاركة **Affiliate programs** والربح الوفير من خلال هذه البرامج
- الحصول على إعلانات ووضعها بموقعك لعمل أرباح كثيرة
- كيفية الحصول على منتجات لبيعها بموقعك
- كيف تسوق موقعك لجذب الزبائن وجلب زوار كثيرة لموقعك

٣- المستوى الثالث

- الإستيراد والتصدير باستخدام شبكة الإنترنت
- كيفية إنشاء شركة إستيراد وتصدير

- إجراءات التصدير والإستيراد والمستندات اللازمة (الشركة–البنك–الجمارك)
- طرق الشحن ووسائل الدفع والتخليص الجمركى
- طرق الحصول على منتجات وأهم المواقع المستخدمة للتصدير والإستيراد

٤- المستوى الرابع

- إستراتيجيات التسويق
- التسويق بواسطة البريد الإليكترونى
- التسويق بواسطة آلات البحث والدلائل
- التسويق بواسطة مواقع إنترنت خاصة بالتجارة الدولية
- التسويق بواسطة المنتديات والقوائم البريدية وبرامج الشات **messenger** و الرسائل القصيرة عبر الإنترنت **sms**

٣- دورات مكملة للتجارة الإليكترونية

١. فوتوشوب **Photoshop** :

- كيفية تصميم بانر **banner** ولوجو وصور المنتجات ببرنامج فوتوشوب
- كيفية تصميم موقع بواسطة برنامج فوتوشوب **Photoshop**

٢. كيفية تصميم موقع بواسطة برنامج باور بوينت **power point**

٣. كيفية تركيب منتدى **Forum** بموقعك وإدارة عمله بواسطة **control panel**

- كيفية عمل القوائم البريدية **mailing list**

للسؤال عن أسعار هذه الدورات والحجز برجاء مراسلتنا

E-mail: scss2004@yahoo.com

scss@books4internet.com

تنبيه هام:

قبل أن تشترى أى كتاب من كتب موسوعة التجارة الإليكترونية تأكد من أن المؤلف هو خالد محمد خالد وذلك لأنه للأسف لوحظ فى الآونة الأخيرة أن أحد دور النشر المعروفة قد سرقت أبواب كاملة من الموسوعه ووضعتها فى كتاب تحت إسم التجارة الإليكترونية ويتم بيعها الآن بالأسواق.وللأسف هذا الكتاب تم نقله بإسلوب غير مفهوم وغير منسق لأنه تم إعداده بمعرفة شخص ليس له علاقة بالتجارة الإليكترونية سوى جنى المال فقط.

المحتويات

الفصل العاشر

الفصل الحادى عشر

الناشر

المركز العلمي لتبسيط العلوم

٢٣ ش رفعت، سيدى بشر، إسكندرية

تليفون : ٥٢٩٨٤٢٨ — فاكس : ٥٢٩٨٤٢٨

International: 0106367467

www.books4internet.com

scss@books4internet.com